WAN Series
Local Management User's Guide
for
Version 2.01.XX Firmware
(specified products only)

WAN Products affected by this manual:	
CSX400	HSIM-W6
CSX400-DC	HSIM-W84
CSX500	

9032672-03

CABLETRON SYSTEMS

Only qualified personnel should perform installation procedures.

NOTICE

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

© 1999 by Cabletron Systems, Inc., P.O. Box 5005, Rochester, NH 03866-5005
All Rights Reserved
Printed in the United States of America

Order Number: 9032672-03 April 1999

Cabletron Systems and **SPECTRUM** are registered trademarks, and **SmartSwitch** is a trademark of Cabletron Systems, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

INDUSTRY CANADA NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements documents (s). The department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas. **Caution:** Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the ringer equivalence Numbers of all the devices does not exceed 5.

VCCI NOTICE

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

CABLETRON SYSTEMS, INC.
PROGRAM LICENSE AGREEMENT

IMPORTANT: THIS LICENSE APPLIES FOR USE OF PRODUCT IN THE FOLLOWING GEOGRAPHICAL REGIONS:

CANADA
MEXICO
CENTRAL AMERICA
SOUTH AMERICA

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between You, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program ("Program") in the package. The Program may be contained in firmware, chips or other media. UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO CABLETRON OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT CABLETRON SYSTEMS (603) 332-9400. Attn: Legal Department.

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

4. EXPORT REQUIREMENTS. You understand that Cabletron and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant o r any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Cabletron and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR IN THE DURATION OR LIMITATION OF IMPLIED WARRANTIES IN SOME INSTANCES, THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.

CABLETRON SYSTEMS SALES AND SERVICE, INC.
PROGRAM LICENSE AGREEMENT

IMPORTANT: THIS LICENSE APPLIES FOR USE OF PRODUCT IN THE UNITED STATES OF AMERICA AND BY UNITED STATES OF AMERICA GOVERNMENT END USERS.

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between You, the end user, and Cabletron Systems Sales and Service, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program ("Program") in the package. The Program may be contained in firmware, chips or other media. UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO CABLETRON OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT CABLETRON SYSTEMS (603) 332-9400. Attn: Legal Department.

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

4. EXPORT REQUIREMENTS. You understand that Cabletron and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant o r any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Cabletron and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR IN THE DURATION OR LIMITATION OF IMPLIED WARRANTIES IN SOME INSTANCES, THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.

CABLETRON SYSTEMS LIMITED
PROGRAM LICENSE AGREEMENT

IMPORTANT: THIS LICENSE APPLIES FOR THE USE OF THE PRODUCT IN THE FOLLOWING GEOGRAPHICAL REGIONS:

EUROPE
MIDDLE EAST
AFRICA
ASIA
AUSTRALIA
PACIFIC RIM

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between You, the end user, and Cabletron Systems Limited ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program ("Program") in the package. The Program may be contained in firmware, chips or other media. UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO CABLETRON OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT CABLETRON SYSTEMS (603) 332-9400. Attn: Legal Department.

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be governed in accordance with English law. The English courts shall have exclusive jurisdiction in the event of any disputes.

4. EXPORT REQUIREMENTS. You understand that Cabletron and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant o r any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component

thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Cabletron and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR IN THE DURATION OR LIMITATION OF IMPLIED WARRANTIES IN SOME INSTANCES, THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.

DECLARATION OF CONFORMITY

Application of Council Directive(s):	**89/336/EEC** **73/23/EEC**
Manufacturer's Name:	**Cabletron Systems, Inc.**
Manufacturer's Address:	**35 Industrial Way** **PO Box 5005** **Rochester, NH 03867**
European Representative Name:	**Mr. J. Solari**
European Representative Address:	**Cabletron Systems Limited** **Nexus House, Newbury Business Park** **London Road, Newbury** **Berkshire RG13 2PZ, England**
Conformance to Directive(s)/Product Standards:	**EC Directive 89/336/EEC** **EC Directive 73/23/EEC** **EN 55022** **EN 50082-1** **EN 60950**
Equipment Type/Environment:	**Networking Equipment, for use in a Commercial or Light Industrial Environment.**

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer	Legal Representative in Europe
Mr. Ronald Fotino	Mr. J. Solari
Full Name	Full Name
Compliance Engineering Manager	Managing Director - E.M.E.A.
Title	Title
Rochester, NH, USA	Newbury, Berkshire, England
Location	Location

Contents

CHAPTER 1 LOCAL MANAGEMENT

Chapter Organization 1-2
WAN Features 1-3
WAN Protocols 1-3
ISDN 1-3
ISDN Call Backup 1-3
Call Backup Topology 1-4
Spoofing 1-5
Local Management Overview 1-5
Management Agent 1-5
Local vs. Remote Management 1-5
Local Management Screen Elements 1-6
Local Management Keyboard Conventions 1-8
Terminal Emulation Setup 1-9
Navigating Within Local Management Screens 1-10
Establishing a TELNET Connection 1-11
Local Management Screen Hierarchy 1-11
Accessing Local Management 1-12
Using the Menu Screens 1-12
Main Menu Screen 1-13
System Level Screen 1-15
Setting the System Date 1-18
Setting the System Time 1-18
Setting the Host IP Address 1-19
Setting the Subnet Mask 1-19
Setting the Default Gateway 1-19
Setting the Default Interface 1-20
SNMP Community Names Screen 1-21
Community Name Access Policy 1-21
Setting SNMP Community Names 1-22

SNMP Traps Screen 1-23
Trap Table Screen Fields 1-23
Setting the SNMP Trap Destination 1-24
Flash Download Screen 1-25
Selecting a Flash Download Method 1-26
Bridge Setup Screen 1-29
Bridge Setup Screen Fields 1-29
Selecting a Spanning Tree Protocol 1-30
Selecting the Bridge Port Administrative Status 1-30
Selecting the Bridge Port Pair Administrative Status 1-31
Router Setup Screen 1-32
Router Setup Fields 1-32
IP Configuration Screen 1-33
IP Configuration Screen Fields 1-33
IP General Configuration Screen 1-34
IP General Configuration Status Fields 1-34
IP General Configuration Fields 1-35
IP RIP 1-40
IP OSPF Configuration 1-45
IPX Configuration Screen 1-48
IPX Configuration Fields 1-48
IPX General Configuration Screen 1-49
IPX General Configuration Status Fields 1-49
IPX General Configuration Fields 1-50
IPX Routing over Frame Relay 1-53
Enabling the IPX SAP Routing Protocol on a Port 1-54
Enabling RIP on a Port 1-55

CHAPTER 2 WAN CONFIGURATION

Chapter Organization 2-1
The WAN Physical Configuration Screen 2-2
WAN Physical Configuration Screen Fields 2-3
HDSL Line Configuration Fields 2-4
T1 Line Configuration Fields 2-5
DDS Line Configuration Fields 2-6
WPIM Timeslot Configuration Table 2-8
WAN Interface Configuration Screen 2-10
WAN Interface Configuration Screen Fields 2-10
Command and Interface Table Fields 2-11
Frame Relay as the Protocol Manager 2-12
PPP as the Protocol Manager 2-13
Remote Profiles Setup 2-14
Remote Profiles Setup Screen Fields 2-14
Bandwidth-on-Demand (Multilink Protocol) Configuration 2-16
Configuration: Full T1 Configuration Using PPP 2-18
T1 Physical Configuration 2-19
T1 Interface Configuration 2-20
Configuration: Fractional T1 Configuration Using PPP 2-21
T1 Physical Configuration 2-22
T1 Interface Configuration 2-23
Configuration: Frame Relay 2-24
Frame Relay Physical Configuration 2-25
Frame Relay Interface Configuration 2-28
Configuration: DDS Service 2-29
DDS Service Physical Configuration 2-30
DDS Service Interface Configuration 2-31
Troubleshooting the Frame Relay Connection 2-32
FR Error Table 2-33

Configuration: Call Backup 2-34
Configure Primary Lines and Routing 2-36
Select the Protocol 2-36
Enable Compression Control Protocol (CCP) 2-38
Configure Backup 2-39
Set Idle Timeouts 2-40
Configure the D Channel 2-41
Set Phone Numbers and SPIDs for the Port 2-41
Set Maximum Number of Neighbor/Remote Profiles 2-42
Configure the Profiles 2-42
Verify Status 2-42
Reset 2-43

CHAPTER 3 MIB NAVIGATOR

Chapter Organization 3-1
MIB Navigator Screen 3-2
Managing Device MIBs 3-2
MIB Navigator Command Set Overview 3-3
Conventions for MIB Navigator Commands 3-5
Navigation Commands 3-6
PPP Security Command 3-14
Spoofing Command 3-14
ISDN Configuration Commands 3-16
Other Commands 3-20
Special Commands 3-35

APPENDIX A WPIM-SY CONFIGURATION

THE WAN PHYSICAL CONFIGURATION SCREEN A-1
WPIM-SY Physical Configuration Fields A-2
WAN Interface Configuration Screen Fields A-3
PPP CONFIGURATION A-4
WPIM-SY Physical Configuration A-4
WPIM-SY Interface Configuration A-5
FRAME RELAY CONFIGURATION A-6
WPIM-SY Physical Configuration A-6
WPIM-SY Interface Configuration A-7

APPENDIX B WPIM-E1 CONFIGURATION

THE WAN PHYSICAL CONFIGURATION SCREEN B-1
WPIM-E1 Configuration Fields B-2
The WPIM Timeslot Configuration Table B-3
THE WAN INTERFACE CONFIGURATION SCREEN B-5
FULL E1 CONFIGURATION USING PPP B-5
WPIM-E1 Physical Configuration B-6
WPIM-E1 Interface Configuration B-7
FRACTIONAL E1 CONFIGURATION USING PPP B-8
WPIM-E1 Physical Configuration B-9
WPIM-E1 Interface Configuration B-10
FRAME RELAY CONFIGURATION B-10
WPIM-E1 Physical Configuration B-11
WPIM-E1 Interface Configuration B-12

APPENDIX C WPIM-DI CONFIGURATION

The WAN Physical Configuration Screen C-1
WPIM-DI Line Configuration Fields C-1
The WAN Interface Configuration Screen C-5
WPIM-DI Configuration C-6
WPIM-DI Physical Configuration C-6
WPIM-DI Interface Configuration C-8

APPENDIX D MODEM SETTINGS FOR RS-232 DIAL-UP PPP BACKUP

FastPro-II Modem Configuration D-2
Origination Modem Configuration D-2
Answer Side Modem Configuration D-3
Courier V.Everything Modem Configuration D-4
Originate (Caller/backup) Side Modem Configuration D-4
Answer Side Modem Configuration D-5

APPENDIX E GLOSSARY

INDEX

1 Local Management

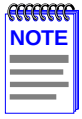
This manual covers Local Management configuration of the CyberSWITCH CSX400, CSX400-DC, and CSX500; and HSIM-W6 and HSIM-W84, as these devices share common component interfaces.

IMPORTANT NOTICE

This manual covers version 02.01.XX or greater, until superseded by a later version manual. For devices running version 01.XX.XX, please refer to the previous manual, part number 9032672-02. This image adds ISDN backup support to the CSX400 and the automatic call backup support for the WPIM-S/T. A major feature of V 2.01.XX FW is the additional mode in Frame Relay so each DLCI can be a MIB II interface. The RFC for Frame Relay DTEs (RFC 2115) is fully supported. The latest version of the ANSI Frame Relay specification is fully supported (ANSI T1-617D 1994). This also changes the FR MIB LMI type to ANSI 1994. Version 2.01.XX also supports RIP2, and the "show" command in MIB Navigation has been updated.

This chapter explains how to access and manage an HSIM or CyberSWITCH and its attached segments through a TELNET connection. WAN Configuration is explained in **Chapter 2**.

A working knowledge of network operations and an understanding of management applications is a prerequisite to using Cabletron Systems Local Management.



The phrase "HSIM or CyberSWITCH" is used in this document to refer to any of the host platforms listed above. In specific cases, the proper name of the host platform is used when referring to something that is particular to that host platform.

Chapter Organization

The following list shows the organization of this chapter:

WAN Features outlines WAN protocols, ISDN, and call backup.

Local Management Overview outlines the contents of this chapter, provides an overview of Local Management, and explains how to use the management screens.

Accessing Local Management describes how to access the Main Menu screen and navigate through the Local Management screens.

System Level Screen describes how to use the System Level screen, its functions, and operations.

SNMP Community Names Screen explains how to control access to an HSIM or CyberSWITCH by assigning community names.

SNMP Traps Screen explains how to configure an HSIM or CyberSWITCH to send SNMP traps to multiple network management stations.

Flash Download Screen describes how to download new firmware to an HSIM or CyberSWITCH.

Bridge Setup Screen describes how to configure an HSIM or CyberSWITCH for bridge functions.

Router Setup Screen describes how to configure an HSIM or CyberSWITCH for bridge functions.

IP Configuration Screen describes how to configure an HSIM or CyberSWITCH for IP routing functions.

IPX Configuration Screen describes how to configure an HSIM or CyberSWITCH for IPX routing functions.

WAN Features

Some of the WAN features are listed and explained here, while others can be found in the *QuickSET Configuration Guide*, which can be found on the QuickSET CD, or on the Cabletron Systems web site for the manuals.

WAN Protocols

The HSIM or CyberSWITCH interface supports ISDN BRI, which encapsulates PPP. For more information, refer to the host platform manual and the Release Notes included with the host platform for a list of current supported protocols.

ISDN BRI is a switched Data Link layer control protocol that uses digital signaling to place a call into an ISDN network. Once the call is made, PPP is then used to transfer data.

PPP is a Data Link layer, industry-standard WAN protocol, used to transfer multi-protocol data traffic over point-to-point connections. With this protocol, options such as security, data compression, and network protocols can be negotiated over the connection.

Frame Relay is a packet-switching data communications protocol that statistically multiplexes many data conversations over a single transmission link. Data compression allows Frame Relay to negotiate compression over Frame Relay PVCs.

ISDN

ISDN provides inexpensive switched digital access to remote sites. The ISDN BRI standard provides for two high-speed 64-Kbps bearer (B) channels used for voice or data connections and one 16-Kbps signaling data (D) channel used for call setup, signaling, and other information. ISDN allows all types of information to be transmitted including voice, data, fax, and video. Multiple devices can be linked to a single ISDN connection, each having their own telephone number. Two or more channels can be combined into a single larger transmission pipe offering variable transmission speeds.

ISDN Call Backup

The ISDN call backup feature provides a backup link for a remote site or branch office when one or more primary WAN interfaces for a frame relay circuit or a nailed-up PPP connection fails. The WPIM-S/T can serve as the backup medium for this primary connection, using the ISDN interfaces to backup any primary interfaces that have been configured for ISDN call backup.

The following are reasons to use ISDN call backup:

- Hardware failure of a nailed-up PPP connection
- line failure

Use call backup if either of the following conditions exist when using Frame Relay:

- DLCI circuit fails to connect in a predetermined amount of time.
- DLCI goes inactive.

The following is one circumstance in which it might not be advisable to use call backup:

- When going point-to-multipoint, setting backup on the head-end side is not recommended. If any DLCI fails, the backup would be activated. This may be cost prohibitive.

Call Backup Topology

In Call Backup topology, two channels are connected, but one of them is a Switched Virtual Circuit (SVC) that is only activated upon failure of the primary channel. The primary channel is a Permanent Virtual Circuit (PVC) running Frame Relay or PPP. The Backup channel is either ISDN BRI or PPP.

Table 1-1 shows the supported configurations at the initial release of the call backup feature.

Table 1-1 Call Backup Configurations

Primary Interface	Backup Interface	Support
PPP (WPIM-T1, WPIM-E1, WPIM-DDS, and WPIM-SY)	ISDN BRI (WPIM-S/T)	**YES**
PPP (WPIM-T1, WPIM-E1, WPIM-DDS, and WPIM-SY)	PPP (WPIM-SY to Sync Modem)	**YES**
Frame Relay (WPIM-T1, WPIM-E1, WPIM-DDS, and WPIM-SY)	ISDN BRI (WPIM-S/T)	**YES**
Frame Relay (WPIM-T1, WPIM-E1, WPIM-DDS, and WPIM-SY)	PPP (WPIM-SY to Sync Modem)	**YES**

Appendix D gives details on a backup configuration using modems.

Spoofing

The concept of mimicking correct responses to keep level requests alive at the local end of a temporarily broken connection is called connection (or call) spoofing. Call spoofing saves connect time charges by allowing the call to be disconnected without causing the NOS to time-out the client/host connection. It also enhances data throughput by keeping the line clear of these network administration packets.

Local Management Overview

Cabletron Systems Local Management is a management tool that allows a network manager to perform the following tasks:

- Configure interconnected devices to form a network.
- Monitor the performance of the network.
- Control user access to the network and its components for the purpose of security.

Management Agent

The management agent is a process within the HSIM or CyberSWITCH that collects information about the operational performance of the managed network. Local Management communicates with the management agent for the purpose of issuing management commands to network devices.

Local vs. Remote Management

Network management applications can be defined as either local or remote applications. A Local Management application resides within the HSIM or CyberSWITCH management agent and is accessible via a TELNET connection through either the EPIM port, or HSIM port of the device.

Remote management applications such as Cabletron Systems **SPECTRUM**, **SPECTRUM Element Manager**, or **QuickSET** run in another device that provides management services. This allows you to perform network management and configuration from a remote location.

Local Management Screen Elements

There are five basic field elements, as shown in the Local Management screen in **Figure 1-1**.

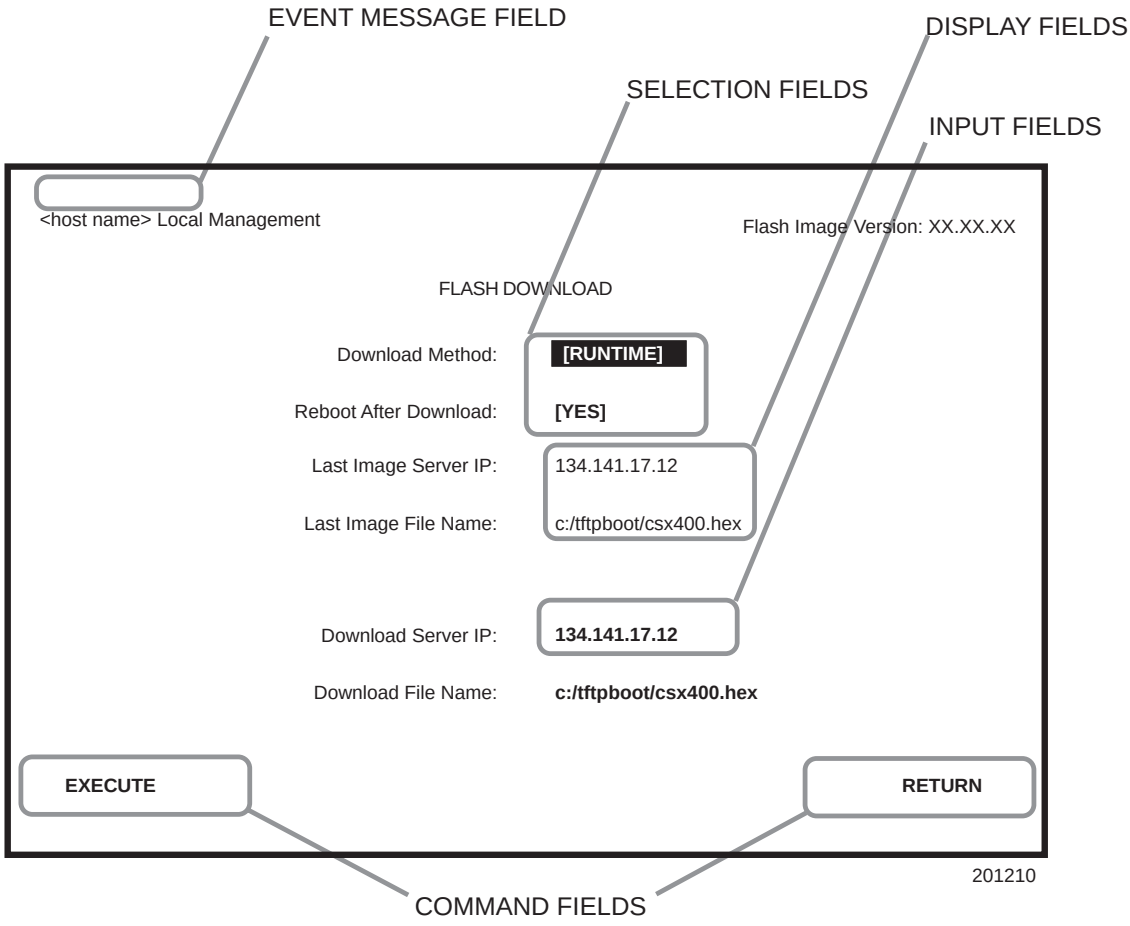


Figure 1-1 Sample Local Management Screen

The following list explains each of the basic Local Management screen fields:

Event Message Field — This field displays messages that indicate if a Local Management procedure was executed correctly or incorrectly, that changes were saved or not saved to Non-Volatile Random Access Memory (NVRAM), or that a user did not have access privileges to an application.

Table 1-2 describes the most common event messages. Event messages related to specific Local Management applications are described with those applications throughout this manual.

Table 1-2 Event Messages

Message	Meaning
SAVED OK	One or more fields were modified, and saved to NVRAM.
NOT SAVED?--PRESS SAVE TO KEEP CHANGES	One or more fields were modified, but not yet saved to NVRAM.
NOTHING TO SAVE	The SAVE command was executed, but nothing was saved to NVRAM.

Display Fields — Display fields cannot be edited. These fields may display information which never changes, or changes as the result of Local Management operations, user selections, or network monitoring information.

Input Fields — Input fields require keyboard characters to be entered. IP addresses, System Date, and System Time are examples of Input fields.

Selection Fields — Selection fields provide a series of possible values. Only applicable values appear in Selection fields.

Command Fields — Command fields are located at the bottom of Local Management screens. Command fields are used to exit Local Management screens and to save Local Management entries. Command fields perform a management action simply by being selected and activated. **Only command fields can make a change to a device's configuration.**

Local Management Keyboard Conventions

All key names in this manual display as capital letters. For example, the ENTER key displays as ENTER, the Escape key displays as ESC, and the Backspace key displays as BACKSPACE. **Table 1-3** explains the keyboard conventions used in this manual as well as the key functions.

Table 1-3 Keyboard Conventions

Key	Function
ENTER and RETURN	These selection keys perform the same Local Management function. For example, “Press ENTER” means that you can press either ENTER or RETURN, unless this manual specifically instructs you otherwise.
ESC	This key lets you escape from a Local Management screen without saving your changes. For example, “Press ESC twice” means that you must quickly press the ESCAPE key two times to exit the Local Management screen.
SPACE bar and BACKSPACE	These keys cycle through selections in some Local Management fields. Press the SPACE bar to cycle forward through selections and press BACKSPACE to cycle backward through selections.
Arrows	These are navigation keys. Use the UP-ARROW, DOWN-ARROW, LEFT-ARROW, and RIGHT-ARROW keys to move the screen cursor. For example, “Use the arrow keys” means to press whichever arrow key moves the cursor to the desired field on the Local Management screen.
SHIFT-[+/=]	This key combination increments values in some Local Management selection fields. For example, “Press SHIFT-[**+/=**]” means to hold down the SHIFT key while pressing the PLUS/EQUAL key.
[–]	This key decreases values from some Local Management selection fields. For example, “Press [**–**]” means to press the MINUS key.
DEL	The DEL (Delete) key removes characters from a Local Management Selection field. For example, “Press DEL” means to press the DELETE key.

Terminal Emulation Setup

You can use QuickSET to initiate a TELNET session if you have no other TELNET application. Your PC's arrow keys are used extensively to navigate within TELNET screens. In order to use the arrow keys effectively for navigating within Local Management screens, you must set your PC up to emulate a Digital Equipment Corporation VT52 terminal.

Start QuickSET and click the **NEXT** button on the first two windows. Under the **File** menu on the title bar of the third window, select **Telnet**. In the title bar of the first Telnet screen, click on **Terminal** and the Terminal menu will display as shown below in **Figure 1-2**.

Click on **Preferences** in the Terminal menu, and the Terminal Preferences window will display as shown below in **Figure 1-2**.

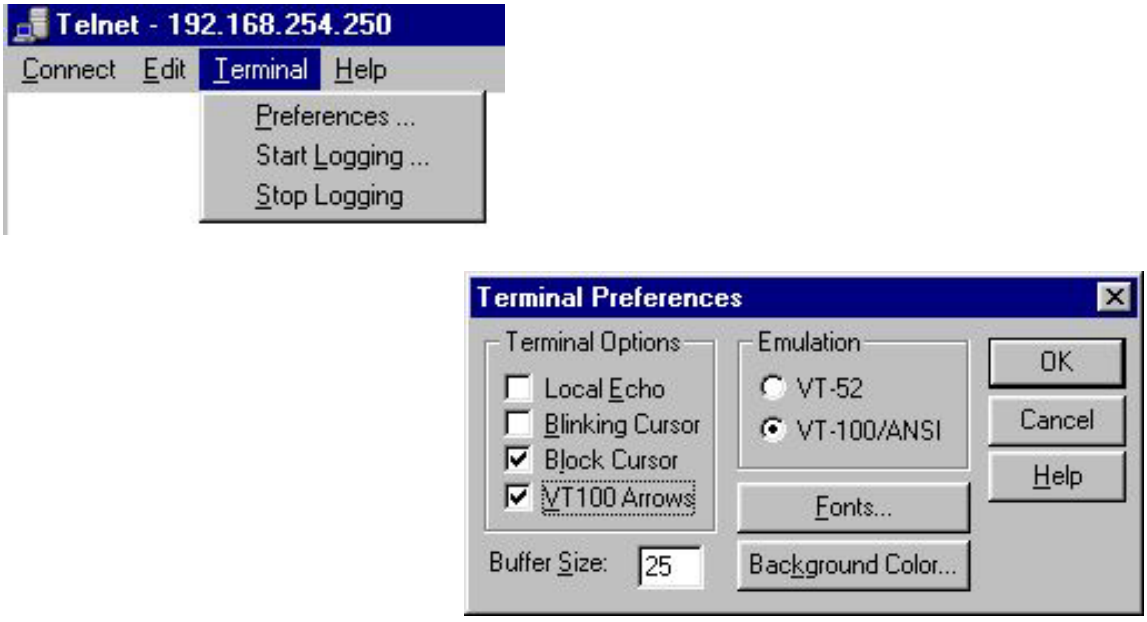


Figure 1-2 Terminal Menu and Terminal Preferences

Select **VT100 Arrows** in the Terminal Options panel, and then select **VT100/ANSI** in the emulation panel if it is not already selected. Click **OK** when you have finished. You are now ready to navigate within any of the Local Management screens.

Navigating Within Local Management Screens

To navigate within a Local Management screen, use the arrow keys of the terminal or the workstation providing terminal emulation services. The Local Management screen cursor responds to the LEFT-ARROW, RIGHT-ARROW, UP-ARROW, and DOWN-ARROW keys. Each time you press an arrow key, the Local Management screen cursor moves to the next available field in the direction of the arrow key.

The Local Management screen cursor only moves to fields which can be selected or used for input. This means that the cursor jumps over display fields and empty lines on the Local Management screen.

The Local Management screen cursor provides wrap-around operation. This means that a cursor located at the edge of a screen, when moved in the direction of that edge, “wraps around” to the outermost selectable item on the opposite side of the screen which is on the same line or column.

Selecting Local Management Menu Screen Items

To select items in a Local Management menu screen, perform the following steps:

1. Use the arrow keys to highlight a menu item.
2. Press **ENTER**. The selected Local Management menu screen displays.

Exiting Local Management Screens

To exit any of the Local Management screens, perform the following steps:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press **ENTER**. The previous screen in the Local Management hierarchy displays.

You can also exit Local Management screens by pressing ESC twice. **This exit method does not warn you about unsaved changes, and all unsaved changes will be lost**.

Exiting the Local Management Session

To exit from HSIM or CyberSWITCH Local Management, perform the following steps:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press ENTER. The previous screen in the Local Management hierarchy displays.

3. Repeat steps 1 and 2 until the Main Menu screen displays.
4. Use the arrow keys to highlight the **EXIT** command at the bottom of the Main Menu screen.
5. Press **ENTER**. The HSIM or CyberSWITCH Local Management Password screen displays and the Local Management session ends.

Establishing a TELNET Connection

The HSIM or CyberSWITCH is shipped with a temporary IP Address of **192.168.254.254** so that your computer can communicate with it over your Local Area Network (LAN) through a TELNET connection. However, to establish a TELNET connection, your computer must be on the same subnet as the HSIM or CyberSWITCH. Cabletron Systems recommends that you assign a temporary IP Address of **192.168.254.253** to your computer to ensure that both devices are on the same subnet. TELNET connections to the host device require the community name passwords assigned at the SNMP Community Names screen or if you are doing an initial configuration, you can use the default password ***public***.

See the instructions included with the TELNET application for information about establishing a TELNET session.

Local Management Screen Hierarchy

Local Management consists of a series of menu screens that provide a path to each of the Local Management function screens. Navigate through Local Management by selecting items from the menu screen. **Figure 1-3** shows the hierarchy of the Local Management screens.

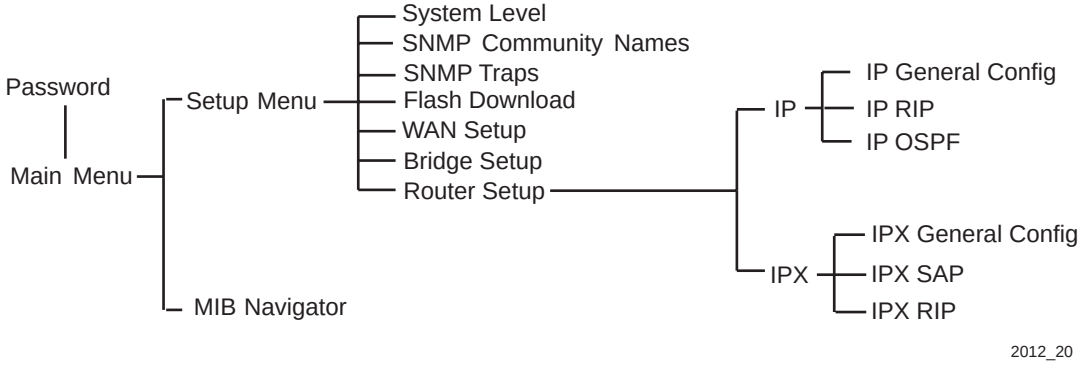


Figure 1-3 Hierarchy of Local Management Screens

Accessing Local Management

This section explains how to access and use the Local Management menu screens. Menu screens provide a path to the setup screens and status screens.

Using the Menu Screens

Once you have accessed the HSIM or CyberSWITCH through a TELNET connection, the Password screen, shown in **Figure 1-4**, displays.

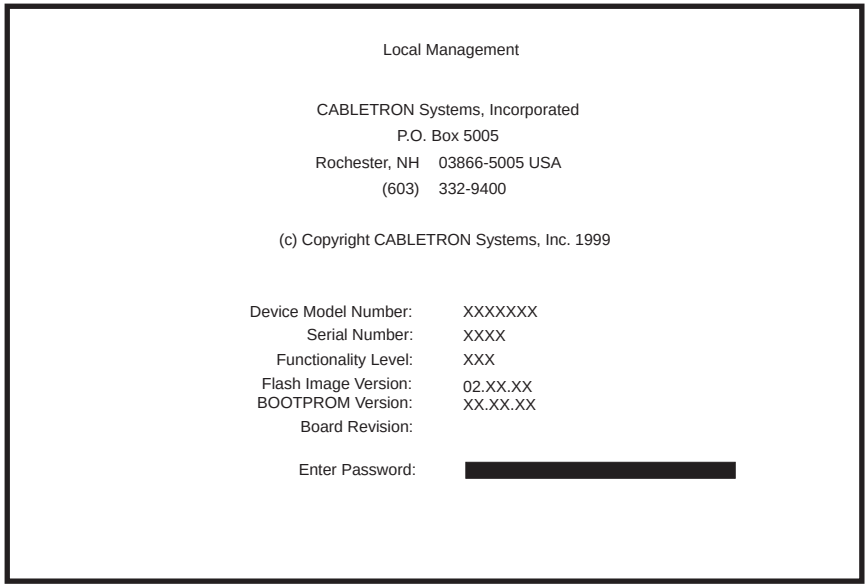


Figure 1-4 Password Screen

Type in your password and press ENTER. If you are doing an initial configuration, you can type the default super-user access password "*public*" or just press ENTER.

NOTE

Your password is one of the community names specified in the SNMP Community Names screen. Access to certain Local Management capabilities depends on the degree of access accorded that community name. See the SNMP Community Names section.

- If you enter a valid password, the associated access level displays at the bottom of the screen and the Main Menu screen, shown in **Figure 1-5**, on the following page, displays.
- If you enter an invalid password, the cursor returns to the beginning of the password entry field.
- If no activity occurs for several minutes, the Password screen displays again, ending your current session. You must reenter the password to perform Local Management tasks.

Main Menu Screen

The Main Menu screen is the starting point from which all the Local Management screens are accessed. **Figure 1-5**, below, shows the Main Menu screen.

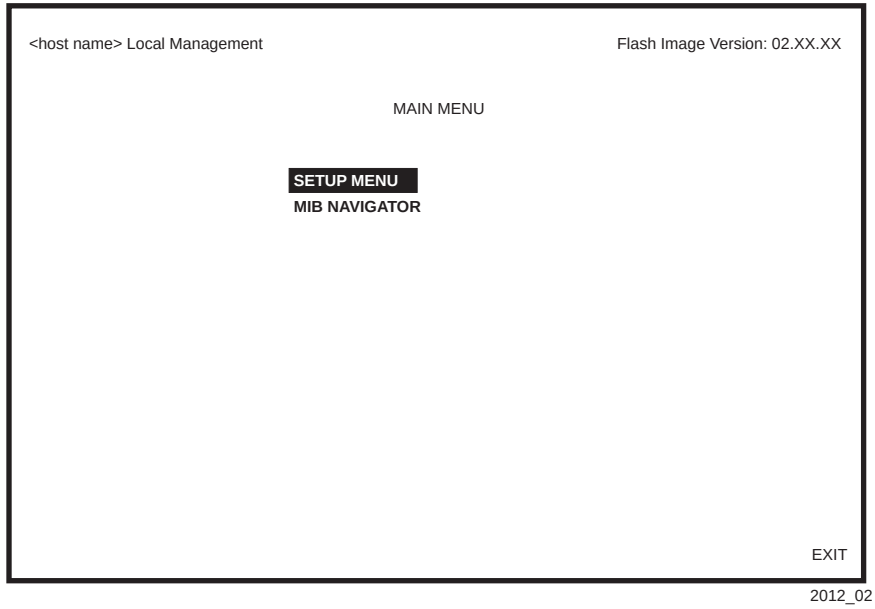


Figure 1-5 Main Menu Screen

The Main Menu screen displays the following menu items:

Setup Menu — The Setup Menu provides access to Local Management screens that are used to configure the HSIM or CyberSWITCH.

MIB Navigator — The MIB Navigator is a Local Management utility that lets you access, monitor, and set specific Management Information Base (MIB) items within the HSIM or CyberSWITCH.

Setup Menu Screen — The Setup Menu screen provides access to the Local Management screens that are used to configure the HSIM or CyberSWITCH. Examples of functions accessible through the Setup Menu include configuring the host IP address and Subnet Mask, assigning the SNMP community names, and configuring the SNMP trap notification. **Figure 1-6** shows the Setup Menu screen.

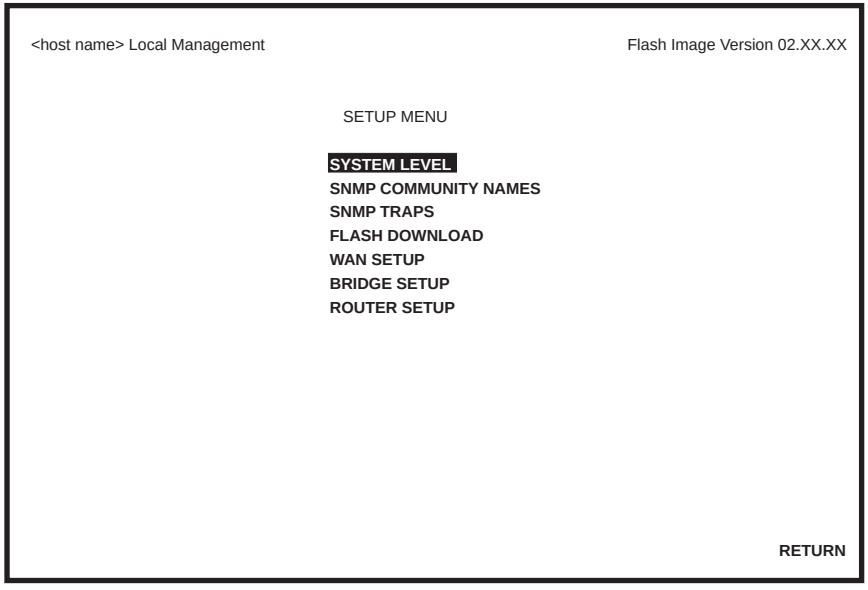


Figure 1-6 Setup Menu Screen

The Setup Menu screen displays the following menu items:

System Level — The System Level screen allows you to configure basic operating parameters for the HSIM or CyberSWITCH.

SNMP Community Names — The SNMP Community Names screen allows you to change or review the community names used as access passwords for local management operation.

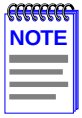
SNMP Traps — The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names.

Flash Download — The Flash Download screen lets you download a firmware image from a TFTP server to the HSIM or CyberSWITCH.

WAN Setup — The WAN Setup menu item accesses two other screens that provide WAN physical configuration and WAN Interface configuration access to enable a WAN link to be set up.

Bridge Setup — The Bridge Setup screen lets you select a Spanning Tree protocol and enable/disable switch ports.

Router Setup — The Router Setup screen accesses two other screens that provide general IP or IPX routing configuration and allow you to enable or disable the Routing Information Protocol (RIP) and the Service Advertising Protocol (SAP) features.



If you have a WPIM-T1, WPIM-DDS, or a WPIM-HDSL installed in your HSIM or CyberSWITCH, refer to the WAN Setup section of this chapter for configuration information. For all other WPIMs, refer to your specific WPIM(s) Local Management Guide or the Appendix for information on configuring the WPIM for a Wide Area Network Interface.

System Level Screen

The System Level screen displays the physical address (MAC address) of the HSIM or CyberSWITCH and allows you to set the following parameters:

- System Date
- System Time
- Host IP Address
- Subnet Mask
- Physical Address
- Default Gateway
- Default Interface

Access the System Level screen (**Figure 1-7**) from the Setup Menu screen by using the arrow keys to highlight the **System Level** option and pressing ENTER. The System Level screen displays.

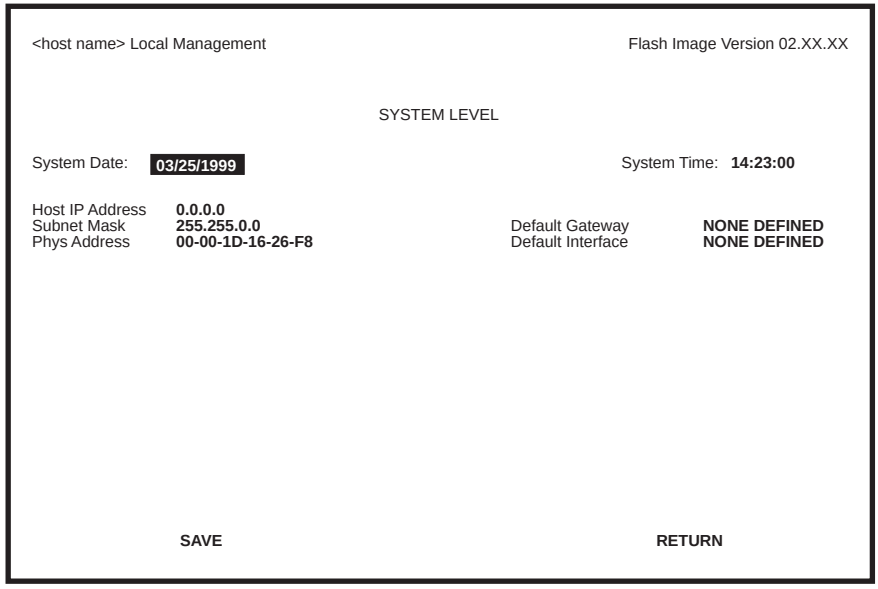


Figure 1-7 System Level Screen

The following definitions explain each System Level screen field. The sections which follow these definitions explain the use of these fields.

System Date — Use this field to enter the system date, as described in **Setting the System Date**.

System Time — Use this field to enter the system time, as described in **Setting the System Time**.

Host IP Address — Use this field to enter the IP address of the HSIM or CyberSWITCH, as described in **Setting the Host IP Address**.

Subnet Mask — This field displays the default Subnet Mask, and allows you to enter a new value for the Subnet Mask if necessary. Subnets are logical divisions of the network that isolate groups of devices. A subnet mask "masks out" the network bits of the IP address by setting the bits in the mask to 1 when the network treats the corresponding bits in the IP address as part of the network or subnetwork address, or to 0 if the corresponding bit identifies the host. The default subnet mask uses the first two portions of the IP address to identify the net id, leaving the rest of the IP address to identify specific nodes.

- When the management workstations designated to receive SNMP traps reside on the same network as the HSIM or CyberSWITCH, use the Subnet Mask default setting for the IP address entered on the System Level screen.
- Set a new value for the Subnet Mask when the management workstations designated to receive SNMP traps reside on a different subnet (for example, across a gateway or router).

To set a Subnet Mask, refer to **Setting the Subnet Mask**.

Phys Address — This field displays the physical address of the HSIM or CyberSWITCH. You cannot modify the physical address.

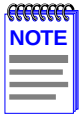
Default Gateway — Use this field to enter the IP address for the Default Gateway, intended for bridging only mode. For routing use a default route entry in your routing table. This field contains the IP address of the device to which all packets addressed to an unknown network or host are sent. The HSIM or CyberSWITCH relies on a Default Gateway to provide the routes to destinations that are not listed in its own IP Forwarding Table, and to forward SNMP traps to a management station. The default setting for this field is NONE DEFINED. To set the Default Gateway, refer to **Setting the Default Gateway**.

Default Interface — Use this field to select the default interface for the HSIM or CyberSWITCH Default Gateway, intended for bridging only mode. For routing use a default route entry in your routing table. The default interface is the channel which is set up to handle SNMP traps sent to an IP station that is not on the same subnet as the HSIM or CyberSWITCH in an IP routed environment. The default setting for this field is NONE DEFINED. To set the default interface for the Default Gateway of the HSIM or CyberSWITCH, refer to **Setting the Default Interface**.

Setting the System Date

The HSIM or CyberSWITCH is year 2000 compliant so that the System Date field can be set beyond the year 1999. To set the system date, perform the following steps:

1. Use the arrow keys to highlight the **System Date** field.
2. Enter the date in an MM/DD/YYYY format.



When entering the date in the system date field, you do not need to add separators between month, day, and year numbers, as long as the entire entry uses eight decimal numbers. For example, to set the date to 06/17/1999, type “06171999” in the System Date field.

3. Press ENTER to set the system date.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered was a valid format, the Event Message field at the top of the screen displays “SAVED OK”. If the entry was not valid, Local Management does not alter the current value and refreshes the System Date field with the previous value.

Setting the System Time

To set the system time, perform the following steps:

1. Use the arrow keys to highlight the **System Time** field.
2. Enter the time in a 24-hour format, HH:MM:SS.

When entering the time in the system time field, you do not need to add separators between hours, minutes, and seconds, as long as each entry uses two decimal numbers. For example, to set the time to 6:45 a.m., type “064500” in the System Time field.

3. Press ENTER to set the system time.
4. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and press ENTER. If the time entered was a valid format, the Event Message field at the top of the screen displays “SAVED OK”. If the entry was not valid, Local Management does not alter the current value and refreshes the System Time field with the previous value.

Setting the Host IP Address

To set the host IP address, perform the following steps:

1. Use the arrow keys to highlight the **Host IP Address** field.
2. Enter the IP address using Decimal Dotted Notation (DDN) format.

   For example: 168.192.25.17
3. Press ENTER. If the IP address entered was a valid format, the cursor returns to the beginning of the Host IP Address field. If the entry was not valid, the Event Message field displays "INVALID IP ADDRESS OR FORMAT ENTERED". Local Management does not alter the current value and refreshes the Host IP Address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays "SAVED OK".

Setting the Subnet Mask

Subnets are logical divisions of the network. To change the Subnet Mask from its default value, perform the following steps:

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the Subnet Mask using Dotted Decimal Notation (DDN) format. Values for each decimal can be from 0 to 255.

   For example: 255.255.0.0
3. Press ENTER. If the Subnet Mask entered was a valid format, the cursor returns to the beginning of the Subnet Mask field. If the entry was not valid, the Event Message field displays "INVALID SUBNET MASK OR FORMAT ENTERED". Local Management does not alter the current value and refreshes the Subnet Mask field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays "SAVED OK".

Setting the Default Gateway

To set the Default Gateway, perform the following steps:

1. Use the arrow keys to highlight the **Default Gateway** field.

2. Enter the IP address of the Default Gateway using DDN format.

   For example: 168.192.79.121

3. Press ENTER. If the Default Gateway address entered was a valid format, the cursor returns to the beginning of the Default Gateway field. If the entry was not valid, the Event Message field displays “INVALID DEFAULT GATEWAY OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Default Gateway field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command field.

5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

The default gateway is intended for bridging only mode. For routing use a default route entry in your routing table.

Setting the Default Interface

To set the default interface, perform the following steps:

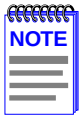
1. Use the arrow keys to highlight the **Default Interface** field.

2. Enter the interface number for the Default Gateway in this field.

3. Press ENTER. If the interface entered was a valid format, the cursor returns to the beginning of the Subnet Mask field. If the entry was not valid, the Event Message field displays “PERMISSIBLE RANGE: 1...X”. Local Management does not alter the current value and refreshes the Default Interface field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command field.

5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.



Both the default gateway and default interface must be changed or an error results. To return to the default state, select NONE DEFINED for both the default gateway and default interface selections.

The default gateway is intended for bridging only mode. For routing use a default route entry in your routing table.

SNMP Community Names Screen

This section explains how to assign community names. Community names allow you to control Local Management access by establishing three passwords. Each password controls a different level of access to HSIM or CyberSWITCH Local Management.

Access the SNMP Community Names screen, shown in **Figure 1-8**, from the Setup Menu screen by using the arrow keys to highlight the **SNMP Community Names** option and pressing ENTER. The SNMP Community Names screen displays.

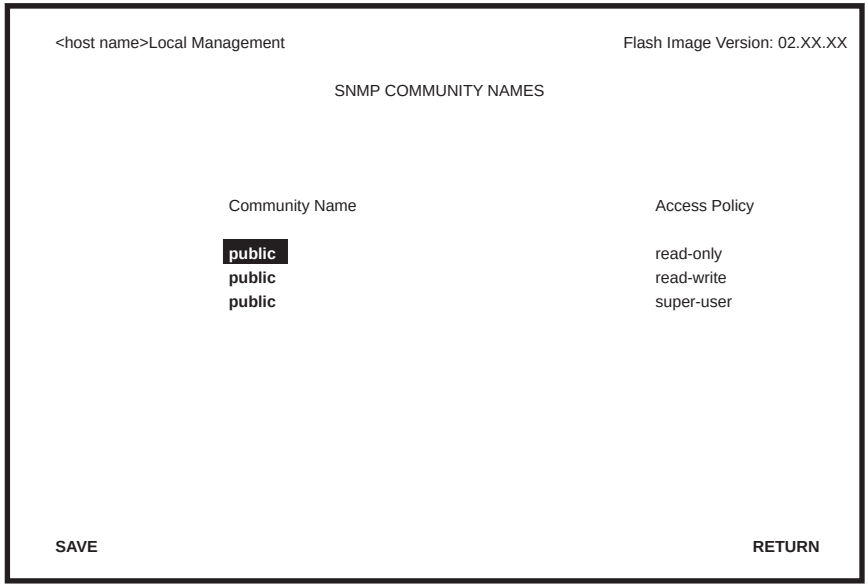


Figure 1-8 SNMP Community Names Screen

Community Name Access Policy

To perform any operations on the SNMP Community Names screen, you must have used the superuser community name at the User Password prompt when initiating the Local Management session. The default community name for each access level is *public*. If you wish to use the default, you can type *public*, or just press ENTER.

The following explains each of the SNMP Community Names screen fields:

Community Name — Displays the user-defined names through which a user accesses the HSIM or CyberSWITCH Local Management. Any community name entered here acts as a password to Local Management.

Access Policy — Indicates the access status accorded each community name. Possible status conditions are:

> **read-only** - This access level allows reading of device parameters not including community names.
>
> **read-write** - This access level allows editing of some device configuration parameters not including changing or viewing community names.
>
> **superuser** - This access level allows full management privileges.

Setting SNMP Community Names

To set a community name, perform the following steps:

If you edit the super-user community name, be certain you do not forget it. If you do, you cannot perform Local Management functions without returning the device to its factory default configurations. This effectively erases any configuration work you have done.

1. Use the arrow keys to highlight the community name you want to change.
2. Type the new community name and press ENTER. The old community name is replaced by the new community name.
3. Use the arrow keys to highlight the **SAVE** command field.
4. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

SNMP Traps Screen

The SNMP Traps screen, shown in **Figure 1-9**, allows the user to configure the HSIM or CyberSWITCH to send traps to as many as eight remote management workstations. SNMP traps are messages about network events and device operational statistics. Access the SNMP Traps screen from the Setup Menu screen by using the arrow keys to highlight the **SNMP Traps** option and pressing ENTER. The SNMP Traps screen displays.

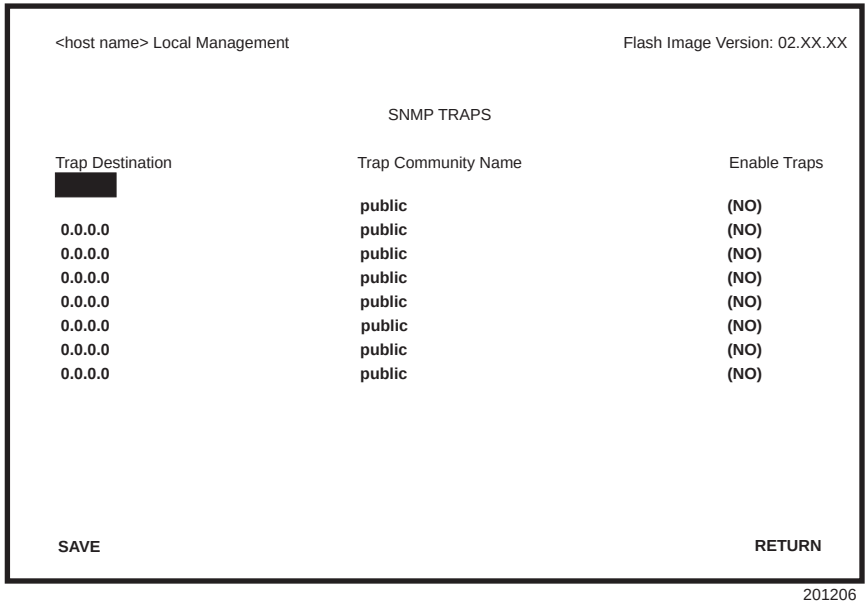


Figure 1-9 SNMP Traps Screen

Trap Table Screen Fields

The following definitions explain each of the SNMP Traps screen fields:

Trap Destination — Use this field to enter the IP address of the management workstation designated to receive SNMP traps from the HSIM or CyberSWITCH.

Trap Community Name — Use this field to enter the community name of the management workstation with the associated IP address. The community name indicates the “access level” of traps that will be forwarded to the Trap destination.

Enable Traps — Use this field to enable the transmission of SNMP traps to the management workstation.

Setting the SNMP Trap Destination

Each management workstation designated to receive SNMP traps from the HSIM or CyberSWITCH must have a valid IP address and community name. To set and enable SNMP trap destination, perform the following steps:

1. Use the arrow keys to highlight the **Trap Destination** field that you want to modify.
2. Type the IP address of the management workstation designated to receive SNMP traps from the HSIM or CyberSWITCH. This address must be entered in DDN format.

   For example: 168.192.25.17
3. Press ENTER. If the IP address entered was a valid format, the cursor returns to the beginning of the Trap Destination IP address field. If the entry was not valid, the Event Message field displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Trap Destination IP address field with the previous value.
4. Use the arrow keys to highlight the **Trap Community Name** field (on the same row as the Trap Destination field).
5. Type the community name of the management workstation. The community name indicates the “access level” of traps that will be forwarded to the Trap destination.
6. Press ENTER.
7. Use the arrow keys to highlight the **Enable Traps** field (on the same row as the Trap Destination and Trap Community Name you have just configured). The default setting for this field is **NO**.
8. Press the SPACE bar or BACKSPACE to set the field to **YES**.
9. Use the arrow keys to highlight the **SAVE** command field.
10. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.
11. Repeat this procedure as necessary to set each Trap Destination.

Flash Download Screen

The Flash Download screen (**Figure 1-10**) allows you to download a firmware image from a TFTP server to the HSIM or CyberSWITCH.

Access the Flash Download screen from the Setup Menu screen by using the arrow keys to highlight the **Flash Download** option and pressing ENTER. The Flash Download screen, shown in **Figure 1-10**, displays.

NOTE

Flash download operations require a properly named download file and a properly configured download server.

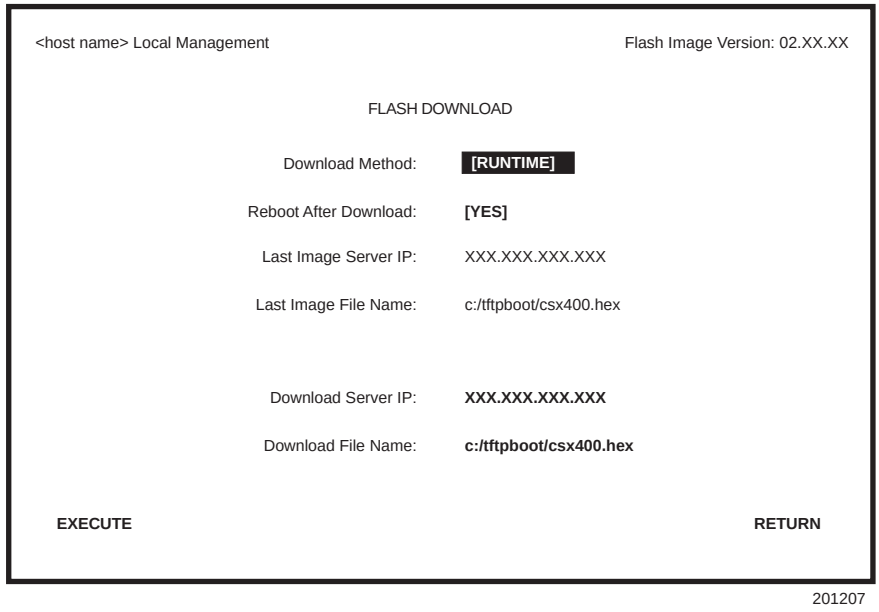


Figure 1-10 Flash Download Screen

The following definitions explain each of the Flash Download screen fields.

Download Method — Use this field to select the method you wish to use to download the firmware image to the HSIM or CyberSWITCH.

- **Reboot After Download —** This field displays when the **RUNTIME** Download Method is chosen. Selecting **YES** forces the HSIM or CyberSWITCH to reboot and use the new firmware image immediately. Selecting **NO** allows the HSIM or CyberSWITCH to continue using the existing firmware image without interrupting network operation.
- **Commit to Flash —** This field displays when the **BOOTPROM** Download Method is chosen. Selecting **YES** allows the HSIM or CyberSWITCH to continue using the existing firmware image without interrupting network operation and selecting **NO** allows the HSIM or CyberSWITCH to reboot and use the new firmware image immediately.
- **TFTP Gateway Server IP —** This field displays when the **BOOTPROM** Download Method is chosen. Use this field to enter the IP address of the TFTP Gateway Server.

Last Image Server IP — Displays the IP address of the last server used to download a firmware image to the HSIM or CyberSWITCH.

Last Image File Name — Displays the file name of the last firmware image downloaded to the HSIM or CyberSWITCH.

Download Server IP — Use this field to type in the IP address of the server from which you wish to download the firmware image.

Download File Name — Use this field to type in the file name of the firmware image you wish to download to the HSIM or CyberSWITCH.

Selecting a Flash Download Method

1. Use the arrow keys to highlight the **Download Method** field.
2. Press the SPACE bar or BACKSPACE to select a flash download method.
   - If you select **RUNTIME**, the Reboot After Download field displays.
   - If you select **BOOTPROM**, the Commit to Flash field and the TFTP Gateway Server IP field display.

RUNTIME Download

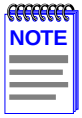
If you select **RUNTIME Download**, perform the following steps:

1. Use the arrow keys to highlight the **Reboot After Download** field.
2. Press the SPACE bar or BACKSPACE to select one of the following:
   - **YES**, if you want the HSIM or CyberSWITCH to reboot and use the new firmware image immediately.
   - **NO**, if you want the HSIM or CyberSWITCH to continue using the existing firmware image without interrupting network operation. The HSIM or CyberSWITCH stores the new firmware image in flash memory. When you reset the HSIM or CyberSWITCH, it boots from flash memory using the new image.
3. Use the arrow keys to highlight the **Download Server IP** field.
4. Type the IP address of the download server and press ENTER.
5. Use the arrow keys to highlight the **Download File Name** field.
6. Type the complete path and filename of the new image file to be downloaded. You must include all directories and subdirectories involved in accessing the file. Type the new entry over the previous entry. For example: c:\images\cyberswitch\11011.hex
7. Press ENTER.
8. Use the arrow keys to highlight the **EXECUTE** command located at the bottom of the Flash Download screen.
9. Press ENTER to begin the download. The HSIM or CyberSWITCH attempts to download the file using the IP address, filename, and path provided. This file is assigned to the Flash memory of the HSIM or CyberSWITCH.

BOOTPROM Download

If you select a **BOOTPROM Download**, perform the following steps:

1. Use the arrow keys to highlight the **Commit to Flash** field.
2. Press the SPACE bar or BACKSPACE to select one of the following:
   - **YES**, if you want the HSIM or CyberSWITCH to continue using the existing firmware image without interrupting network operation. The HSIM or CyberSWITCH stores the new firmware image in flash memory. When you reset the HSIM or CyberSWITCH, it boots from flash memory using the new image.
   - **NO**, if you want the HSIM or CyberSWITCH to reboot and use the new firmware image immediately.
3. Use the arrow keys to highlight the **Download Server IP** field.
4. Type the IP address of the download server and press ENTER.
5. Use the arrow keys to highlight the **Download File Name** field.
6. Type the complete path and filename of the new image file to be downloaded. You must include all directories and subdirectories involved in accessing the file. Type the new entry over the previous entry. For example: c:\images\cyberswitch\11011.hex.
7. Press ENTER.
8. Use the arrow keys to highlight the **TFTP Gateway Server IP** field.
9. Enter the IP address of the TFTP gateway server.
10. Use the arrow keys to highlight the **EXECUTE** command located at the bottom of the Flash Download screen. The HSIM or CyberSWITCH attempts to download the file using the IP address, filename, and path provided. This file is assigned to the Flash memory of the HSIM or CyberSWITCH.



The WAN Setup portion of Local Management is detailed in **Chapter 2, WAN Configuration**.

Bridge Setup Screen

The Bridge Setup screen enables you to select a Spanning Tree protocol and enable/disable bridge ports. Access the Bridge Setup screen, shown in **Figure 1-11**, by using the arrow keys to highlight the **Bridge Setup** option and pressing ENTER. The Bridge Setup screen displays.

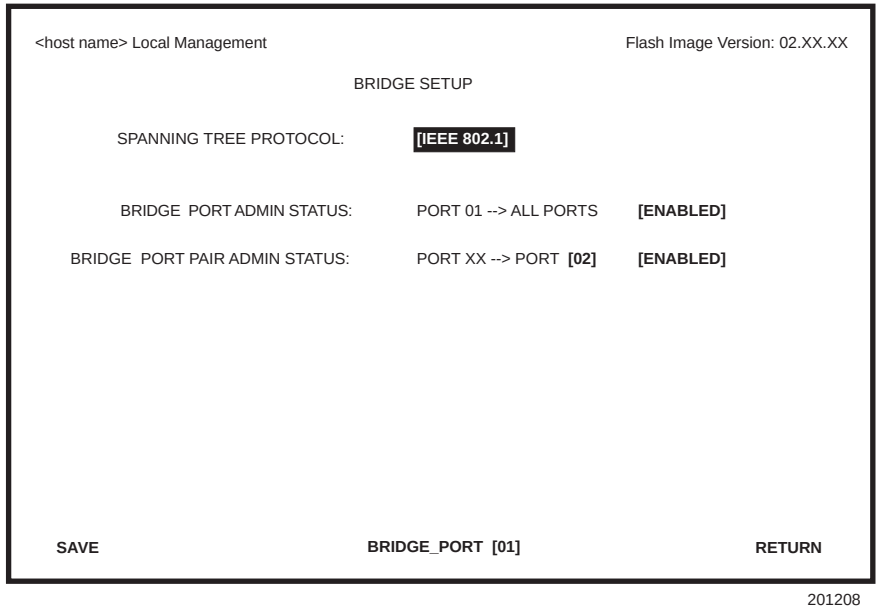


Figure 1-11 Bridge Setup Screen

Bridge Setup Screen Fields

The following list describes each of the Bridge Setup screen fields:

SPANNING TREE PROTOCOL — Use this field to select a Spanning Tree protocol. Possible selections for this field are IEEE 802.1, DEC, or NONE.

BRIDGE PORT ADMIN STATUS — Use this field to enable or disable individual HSIM or CyberSWITCH bridge ports. Possible selections for this field are ENABLED or DISABLED.

BRIDGE PORT PAIR ADMIN STATUS — Use this field to enable or disable bridging between bridge port pairs. For example, you can enable Port 1 to bridge traffic to all ports except Port 2.

BRIDGE_PORT *XX* — Use this command field to select the HSIM or CyberSWITCH bridge port you want to configure.

Selecting a Spanning Tree Protocol

To select the Spanning Tree protocol to be used by the HSIM or CyberSWITCH, perform the following steps:

1. Use the arrow keys to highlight the **SPANNING TREE PROTOCOL** field.
2. Press the SPACE bar or BACKSPACE to select **[IEEE 802.1]**, **[DEC]**, or **[NONE]**.
3. Use the arrow keys to highlight the **SAVE** command field.
4. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Selecting the Bridge Port Administrative Status

To select the bridge port administrative status, perform the following steps:

1. Use the arrow keys to highlight the **[BRIDGE_PORT *XX*]** field at the bottom of the Bridge Setup screen.
2. Press the SPACE bar or BACKSPACE to select the bridge port you want to configure. The selected bridge port displays in the Bridge Port Admin Status field.
3. Use the arrow keys to highlight the **BRIDGE PORT ADMIN STATUS: PORT X - - > ALL PORTS [ENABLED]** field.
4. Press the SPACE bar or BACKSPACE to select **ENABLE** or **DISABLE**.

   For example, the following bridge setup indicates that bridge port 01 is configured to bridge traffic to all ports:

   BRIDGE PORT ADMIN STATUS: PORT **01** - - > ALL PORTS **[ENABLED]**
5. Use the arrow keys to highlight the **SAVE** command field.
6. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Selecting the Bridge Port Pair Administrative Status

To select the bridge port pair administrative status, perform the following steps:

1. Use the arrow keys to highlight the **[BRIDGE_PORT *XX*]** field at the bottom of the Bridge Setup screen.
2. Press the SPACE bar or BACKSPACE to select the bridge port you want to configure. The selected bridge port displays in the Bridge Port Pair Admin Status field.
3. Use the arrow keys to highlight the **BRIDGE PORT PAIR ADMIN STATUS: PORT X - -> PORT [Y]** field.
4. Press the SPACE bar or BACKSPACE to select the port you want to enable or disable bridge traffic.
5. Use the arrow keys to highlight the **BRIDGE PORT PAIR ADMIN STATUS: PORT X - -> PORT [Y] [ENABLED]** field.
6. Press the SPACE bar or BACKSPACE to select **ENABLE** or **DISABLE**.

   For example, the following bridge setup indicates that bridge port 01 is configured NOT to bridge traffic to bridge port 02:

   BRIDGE PORT PAIR ADMIN STATUS: PORT **01** - - > PORT **[02] [DISABLED]**
7. Use the arrow keys to highlight the **SAVE** command field.
8. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Router Setup Screen

The Router Setup menu screen allows you to choose either IP or IPX routing for your HSIM or CyberSWITCH.

Access the Router Setup screen, shown in **Figure 1-12**, by using the arrow keys to highlight the **ROUTER SETUP** menu item in the Setup Menu and pressing ENTER. The Router Setup menu screen displays.

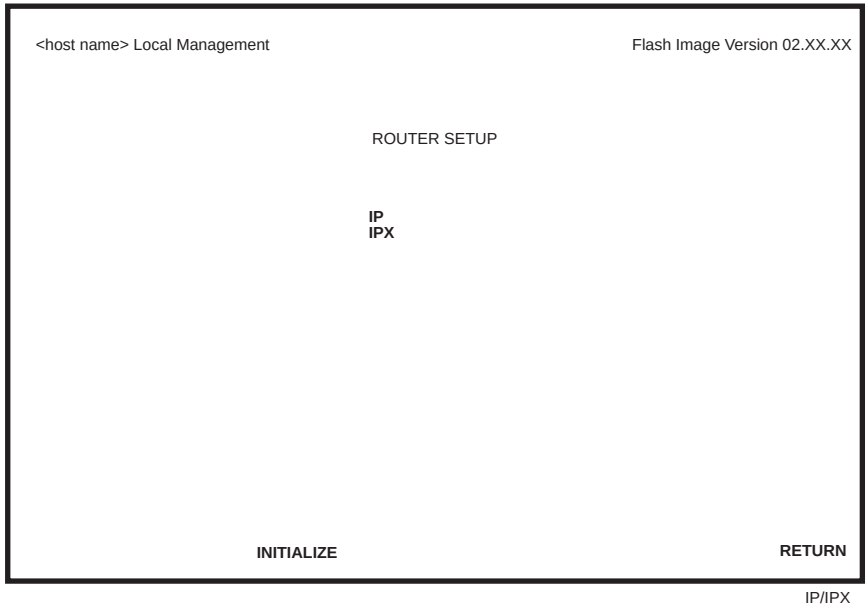


Figure 1-12 Router Setup Screen

Router Setup Fields

The following list describes the Router Setup menu screen.

IP — Use this field to access the **IP Configuration Screen** to configure the HSIM or CyberSWITCH for IP routing.

IPX — Use this field to access the **IPX Configuration Screen** to configure the HSIM or CyberSWITCH for IPX routing.

INITIALIZE — The device does a soft reset to allow any setting changes to be saved, no diagnostics are performed.

IP Configuration Screen

The IP Configuration menu screen enables you to access the IP General Config and IP RIP screens to configure the HSIM or CyberSWITCH for IP Routing and enable RIP on the HSIM or CyberSWITCH.

Access the IP Configuration menu screen, shown in **Figure 1-13**, by using the arrow keys to highlight the **IP** menu item on the Router Setup screen and pressing ENTER. The IP Configuration screen displays.

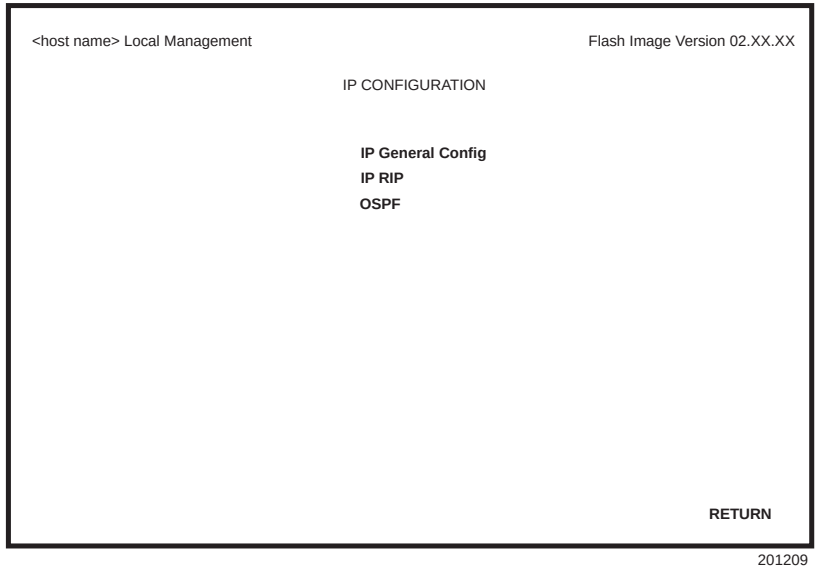


Figure 1-13 IP Configuration Screen

IP Configuration Screen Fields

The following list describes each of the IP Configuration screen fields.

IP General Config — Use this field to access the **IP General Configuration Screen** and configure the HSIM or CyberSWITCH for IP routing.

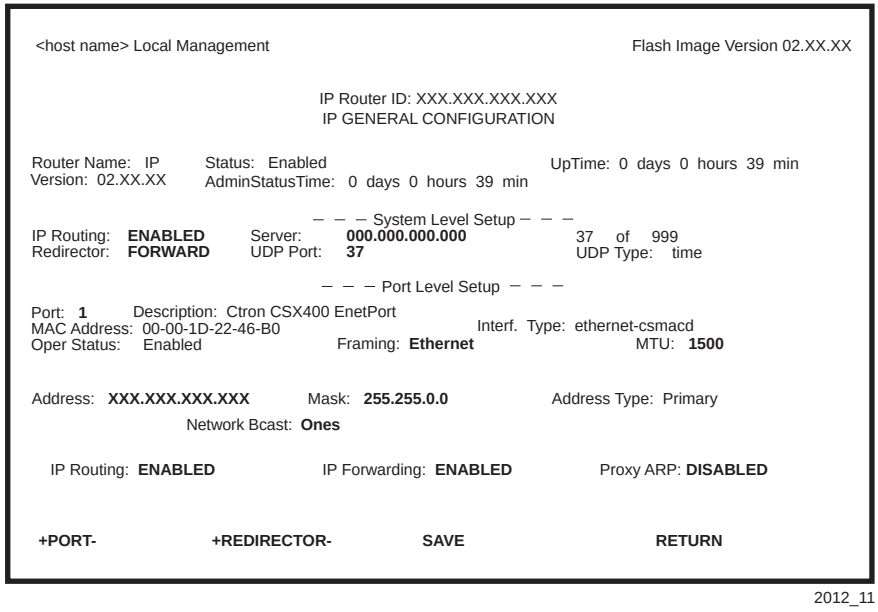
IP RIP — Use this field to access the **IP RIP** screen and enable Routing Information Protocol (RIP) routing on the HSIM or CyberSWITCH.

IP OSPF — Use this field to access the **IP OSPF Configuration** screen to configure and enable OSPF for IP routing on the HSIM or CyberSWITCH.

IP General Configuration Screen

The IP General Configuration screen allows you to configure the HSIM or CyberSWITCH for IP routing.

Access the IP General Configuration screen by using the arrow keys to highlight the **IP General Config** menu item and pressing ENTER. The IP General Configuration screen shown in **Figure 1-14** displays.



2012_11

Figure 1-14 IP General Configuration Screen

IP General Configuration Status Fields

The following list describes each of the IP General Configuration status fields. The status fields are for informational purposes only and cannot be modified.

Router Name — Displays the type of routing used.

Status — Displays the status of IP Routing.

UpTime — Displays the amount of time elapsed since the last time the HSIM or CyberSWITCH was rebooted.

Version — Displays the IP Routing version number used on the HSIM or CyberSWITCH.

AdminStatusTime — Displays the amount of time elapsed since an IP address was assigned to the HSIM or CyberSWITCH.

UDP Type — Displays the User Datagram Protocol (UDP) Service to which the selected UDP Port number corresponds.

Description — Describes the selected Port.

MAC Address — Displays the physical (MAC) address of the HSIM or CyberSWITCH.

Interf. Type — Displays the type of interface used by the specified port.

Oper Status — Displays the operational status of the selected port.

IP General Configuration Fields

This section provides a general overview of the procedures required to configure the HSIM or CyberSWITCH. The following describes each of the modifiable IP General Config Screen fields.

+PORT- — Use this field to select the routing port you wish to configure.

+REDIRECTOR- — Use this field to toggle through a list of commonly used UDP port numbers. UDP port numbers are associated with the relay agent functionality of the router.

UDP Port — User Datagram Protocol (UDP) Port affected.

Framing — Use this field to select the format of the frame in which IP packets are encapsulated for transmission.

MTU — Use this field to set the Maximum Transmission Unit (MTU).

IP Routing — Use this field to enable IP Routing Services.

IP Forwarding — Use this field to enable IP Forwarding.

Proxy ARP — Use this field to enable Proxy Address Resolution Protocol (ARP).

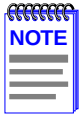
Address — Use this field to assign an IP address to the port that you wish to configure.

Mask — Use this field to set the Subnet Mask for the port that you wish to configure.

Selecting a Port for Configuration

Routing Services allows you to choose the ports that you want to configure for IP routing. To select a router port to configure for IP routing, complete the following steps:

1. Use the arrow keys to highlight the **PORT** option.
2. Type in the number of the port that you want to configure for IP routing and then press ENTER.



You can type in the port number, or you can use the +**PORT**- option at the bottom of the screen to scroll through the list of the ports on your device. To use the +**PORT**- option, use the arrow keys to highlight the + (to go forward), or the - (to go backward), and then press **ENTER** to scroll through the available ports in the direction you have selected. You can also use the **+** and **-** keys to scroll through the available ports.

If you type in an invalid port number, the error message “PORT NUMBER IS OUT OF RANGE” displays. Perform steps 1 and 2 again.

Entering the IP Address and Subnet Mask

All IP hosts must have an IP Address for each network interface. These addresses identify each network connection.

To enter the IP address for a router port, complete the following steps:

1. Use the arrow keys to highlight the **ADDRESS** option.
2. Type in the IP address and then press ENTER.

Once an IP address is entered, the default Subnet Mask automatically enters into the Mask field. To to change the default Subnet Mask for a router port, complete the following steps:

1. Use the arrow keys to highlight the **MASK** option.
2. Type in the Subnet Mask for the IP address that you have assigned.

Selecting the Frame Type for a Port

On each port, Frame Type specifies the format of the frame in which IP packets are encapsulated for transmission. The Frame Type options available for each router port are dependent on the type of media supported by that router port. The choices are: Ethernet, SNAP, i8022, Novell, Localtalk, Native-wan, Encap-enet, Encap-enet-8022, Encap-enet-snap, Encap-enet-novell, Encap-tokenring-8022, Encap-tokenring-snap, Encap-fddi-8022, Encap-fddi-snap, Other.

Select the Frame Type based on your implementation, for example: Native-wan for router to router communication, and Encap-enet or Encap-enet-snap can be chosen for either router to bridge, or bridge to bridge communication.

To select the Frame Type for a port, complete the following steps:

1. Use the arrow keys to highlight the **Framing** option.
2. Use the ENTER key to toggle the entry to the correct Frame Type for the port.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Setting the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit specifies the maximum packet size for all IP packets that are transmitted.

To select the MTU for a port, complete the following steps:

1. Use the arrow keys to highlight the **MTU** option under Port Level Setup.
2. Enter an MTU value for the media used.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, then press ENTER. The message “SAVED OK” displays.

Enabling IP Routing Services on a Port

The ability to switch IP Routing Services on and off on a port-by-port basis, provides great flexibility. On the same device, some ports can be routing IP traffic while other ports are bridging it. As you are in transition from a bridged network to a routed network, this flexibility allows you to implement IP routing and test your routing configuration on a port-by-port basis. If necessary, you can temporarily disable the IP routing on any port without losing your configuration, or you can temporarily switch from IP routing back to bridging.

To enable IP Routing Services on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IP Routing** option under Port Level Setup.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.

Enabling IP Forwarding on a Port

By default, IP Forwarding is disabled on each router port. Your device cannot begin forwarding IP data packets on any router port until you enable IP Forwarding on that port.

To enable IP Forwarding on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IP Forwarding** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message "SAVED OK" displays.

Configuring the UDP Broadcast Redirector

To locate a server that can provide a particular network service, many IP hosts rely on the use of LAN broadcasts to send UDP service requests. The UDP port number contained in the broadcast request packet identifies the service being requested. Table 1-4 shows the port numbers and their corresponding requested services.

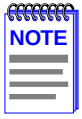
Table 1-4 UDP Port Numbers

UDP Port #	UDP Services
37	Time
42	Host Name Server
53	Domain Name Server
65	TACACS-Database Service
67	Bootstrap Protocol/Dynamic Host Control Protocol Server
68	Bootstrap Protocol/Dynamic Host Control Protocol Client
69	Trivial File Transfer
137	NETBIOS Name Server
138	NETBIOS Datagram Server
111	Sunrpc (NIS)

The UDP Broadcast Redirector enables you to configure any Routing Services enabled device to forward the UDP packets that it receives as LAN broadcasts, directly to the appropriate server. UDP service requests that are sent as LAN broadcasts by clients of applications such as Host Name, Domain Name, and Bootstrap servers, can be redirected to any server on any network segment.

To configure the UDP Broadcast Redirector, complete the following steps:

1. Use the arrow keys to highlight the **UDP Port** option under System Level Setup.
2. Enter the UDP port number of the UDP service request packets that you want to redirect (refer to **Table 1-4**) and then press ENTER.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message "SAVED OK" displays.



You can type in the UDP port number, or you can use the +**REDIRECTOR**- option at the bottom of the screen to scroll through a list of commonly used UDP port numbers. To use the +**REDIRECTOR**- option, use the arrow keys to highlight the + (to go forward), or the - (to go backward), and then press the **ENTER** key to scroll in the direction that you selected.

The entry for the UDP Port option reflects the UDP port number that is currently selected. The entry for UDP Type names the UDP service to which that port number corresponds.

Enabling Proxy ARP on a Port

By default, Proxy Address Resolution Protocol (ARP) is disabled on all ports, and IP Routing Services respond only to ARP requests addressed to its own IP address.

For one IP host to communicate with another IP host, knowledge of the target host's MAC address must be known. To learn this MAC address, the IP host sends an ARP request packet as a LAN broadcast with the destination IP address of the target IP host. All hosts receive this broadcast and the one host that matches the target IP address responds with its MAC-layer address.

However, because each subnet constitutes a separate broadcast domain and LAN broadcasts are not forwarded across routers, ARP does not work beyond a host's local network or subnetwork. One of the primary purposes of a router is to confine LAN broadcast traffic to each local network or subnetwork.

A proxy ARP response is generated when the following occurs:

- Proxy ARP is enabled on a router port.
- An ARP request is received as a LAN broadcast (looking for the MAC-layer address of an IP host on another network segment).
- An entry exists in the IP Forwarding Table for the destination host's network.

Enabling Proxy ARP on a router port allows IP hosts to dynamically obtain the MAC-layer address of other IP hosts attached to different networks or subnetworks by using broadcast ARP request packets. With Proxy ARP enabled, IP hosts are not required to maintain knowledge of specific subnetworks.

To enable Proxy ARP on a router port, complete the following steps:

1. Use the arrow keys to highlight the **Proxy ARP** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message "SAVED OK" displays.

Configuring the Network Broadcast Type on a Port

IP Routing Services recognizes and accepts network broadcasts, IP packets with the host portion of the IP address as either all 1's or all 0's. Other networking devices only recognize all 0's as a network broadcast.

To configure IP Routing Services to send network broadcasts addressed to all 0's, complete the following steps:

1. Use the arrow keys to highlight the **Network Bcast** option.
2. Use the ENTER key to toggle the entry to **ZEROS**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message "SAVED OK" displays.

IP RIP

Routing Information Protocol (RIP) is a widely implemented routing protocol that is used extensively on IP internetworks. IP Routing Services uses the RIP routing protocol to send and gather information about the internetwork topology. This information is used to construct and maintain a database called RIP Route Table, which contains the addresses of the available routes to all the networks and hosts that RIP has learned.

Enabling the RIP routing protocol allows IP Routing Services to build and maintain a dynamic database of route information. The best routes learned by the RIP routing protocol are added to the IP Forwarding Table to forward IP packets. The ability to switch the RIP routing protocol on and off on a port-by-port basis provides great flexibility. On the same device, some router ports can be running the RIP routing protocol while other router ports are not. If necessary, you can temporarily disable the RIP routing protocol on any port without affecting the rest of your configuration.

RIP-2

The following definitions compare and contrast some of the features of the RIP-1 and RIP-2 protocols.

RIP-1 vs. RIP-2 — A comparison of the features of RIP-1 and RIP-2 protocols (excerpted from RFC 1722, and RFC 2080) follows:

RIP-2 is essentially an extension of RIP-1; it is not a new protocol. It is a superset of the environments in which RIP-1 has been traditionally used. It should be noted that RIP-2 is not intended to be a substitute for OSPF (Open Shortest Path First) protocol in large autonomous systems. The restrictions on autonomous system diameter and complexity which applied to RIP-1 also apply to RIP-2.

Subnet Masks — RIP-2 allows the smaller, simpler, distance-vector protocol to be used in environments that require authentication or the use of variable length subnet masks, but are not of a size or complexity that requires the use of the larger, more complex link-state OSPF protocol.

The original impetus behind the creation of RIP-2 was the desire to include subnet masks in the routing information exchanged by RIP, as this was not included in the original definition of RIP. As long as the subnet mask was fixed for a network, and well known by all the nodes on that network, a heuristic could be used to determine if a route was a subnet route or a host route.

The inclusion of the subnet mask in RIP-2 effectively creates a 64-bit address, which eliminates the network, subnet, and host distinction. Therefore the inclusion of a subnet mask in RIP-2 allows it to be used in an autonomous system which requires precise knowledge of the subnet mask for a given route, but does not otherwise require OSPF protocol.

Next Hop — Entries in RIP-2 routing tables always have a Next Hop field. The Next Hop is the IPv6address of the next router along the path to the destination. The purpose of the Next Hop in the routing table is to prevent packets from being routed through extra hops in the system. The limitation of a maximum network diameter of 15 hops for the Next Hop field is common to both RIP-1 and RIP-2. This statement of the limit assumes that a cost of 1 is used for each network (see Metrics, below).

Metrics — The RIP-1 and RIP-2 protocols use fixed “metrics” to compare alternative routes. This is not appropriate where routes need to be chosen based on real-time parameters such as measured delay, reliability, or load. RIP is intended to allow routers to exchange information for computing routes through an IPv6-based network. Any router that uses RIP is assumed to have interfaces to one or more networks, otherwise it isn’t a router. These are referred to as directly connected networks.

The RIP protocol relies on access to certain information about each of these networks, the most important of which is its metric. This metric represents the total “cost” of getting a datagram from the router to that destination.

The routing table has the entries listed below for each destination that is reachable:

- The IPv6 prefix of the destination
- A metric, described above
- The IPv6 address of the next router along the path (the Next Hop)
- A flag to indicate the information about the route has changed recently
- Various timers associated with the route

Split Horizon — Split Horizon is an algorithm for avoiding problems caused by including routes in the updates sent to the gateway from which they were learned. The basic split horizon algorithm omits routes learned from one neighbor in updates sent to that neighbor.

Authentication — Authentication is a function of RIP-2 protocol only. It is not usually important to conceal the information in the routing messages, but it is essential to prevent the insertion of bogus routing information into the routers. Authentication prevents someone who cannot directly access the network (i.e., someone who cannot sniff the packets to determine the password) from inserting bogus routing information. Currently the authentication type is simple password and MD5.

Multicasting — The RIP-2 protocol provides for the IP multicasting of periodic advertisements. This feature was added to RIP-2 to decrease the load on systems that do not support RIP-2. It also provides a mechanism whereby RIP-1 routers will never receive RIP-2 routes. This feature is useful when the correct use of an advertised route depends on knowing the precise subnet mask, which would be ignored by a RIP-1 router.

Compatibility Switch — A compatibility switch is necessary for two reasons. First, there are implementations of RIP-1 in the field that do not follow RFC1058, and second, the use of multicasting would prevent RIP-1 systems from receiving RIP-2 updates (which may be a desired feature in some cases). This switch is configurable on a “per-interface” basis.

The switch has four send settings:

- RIP-1, in which only RIP-1 messages are sent (and received)
- RIP-1 Compatible, in which RIP-2 messages are broadcast
- RIP-2, in which RIP-2 messages are multicast
- DON’T SEND, which disables the sending of all RIP messages

The receive control has four settings:

- RIP1, only accept RIP-1 messages
- RIP2, only accept RIP-2 messages
- RIP1/RIP2, accept both RIP-1 and RIP-2 messages
- DON’T RCV, do not accept any type of RIP messages

This control is also configurable on a “per-interface” basis.

If the router is not configured to authenticate RIP-2 messages, then RIP-1 and unauthenticated RIP-2 messages will be accepted. Authenticated RIP-2 messages will be discarded. If the router is configured to authenticate RIP-2 messages, then RIP-1 messages and RIP-2 messages which pass authentication testing will be accepted. Unauthenticated and failed authentication RIP-2 messages shall be discarded.

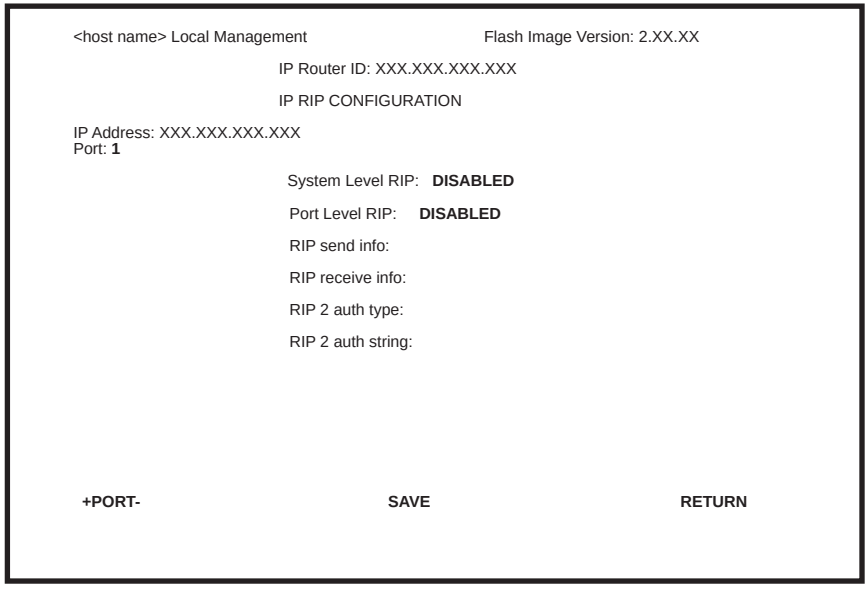


Figure 1-15 IP RIP Configuration Screen

To enable RIP Routing, complete the following steps:

1. From the IP Configuration screen, highlight **IP RIP** and then press ENTER.

   The IP RIP Configuration screen, shown in **Figure 1-15**, displays.

2. Use the arrow keys to highlight the **System Level RIP** option.
3. Use the ENTER key to toggle the entry to **ENABLED**.
4. Use the arrow keys to highlight the **Port Level RIP** option.
5. Use the ENTER key to toggle the entry to **ENABLED**.
6. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.
7. Exit back out to the Router Setup screen, use the arrow keys to highlight the INITIALIZE command, and use the ENTER key to initialize the device. The connection to Local Management will disconnect and re-entry is necessary for any further configuration. Access the IP RIP Configuration screen as before in order to continue configuration.
8. Use the arrow keys to highlight the **RIP send info** option.

9. Use the ENTER key to toggle the entry. RIP1 is the default, the other choices are RIP2, DON'T SEND, and RIP1 COMPATIBLE. Make the proper selection for your network.
10. Use the arrow keys to highlight the **RIP receive info** option.
11. Use the ENTER key to toggle the entry. RIP1 is the default, and the other choices are RIP2, RIP1/RIP2, and DON'T RCV.
12. Use the arrow keys to highlight the **RIP2 auth type** option.
13. Use the ENTER key to toggle the entry. NONE is the default, and the other choices are PASSWORD and MD5.
14. If PASSWORD or MD5 is chosen, the next selection is the user defined choice of the password in the RIP2 auth string field. Use the arrow keys the highlight the **RIP2 auth string** field.
15. The password, up to 16 characters in length, may be entered here.
16. The **+PORT-** command can be used to go to the next available port, when there is a port configured. Use the SPACE bar to advance to the next port for configuration. Repeat the entire procedure as above in order to configure the new selected port.

IP OSPF Configuration

OSPF (Open Shortest Path First) is a Link-State Protocol. OSPF distributes routing information between routers belonging to a single Autonomous System (AS). In an Autonomous System, routers exchange routing information through a common routing protocol.

An Autonomous System may contain one or more networks, but each network within the AS may or may not support subnetting. Every OSPF routing domain must have a "Backbone". An OSPF backbone distributes routing information between areas in an OSPF routing domain. The backbone of an OSPF routing domain is an OSPF area possessing an area ID of 0.0.0.0. Because OSPF protocol only broadcasts link state updates when topology has changed, it is considered "quiet" when compared to RIP protocol, which has to periodically send a portion, or all of its routing table to its neighbors.

Convergence (the time it takes to recalculate routing tables) under OSPF protocol is instantaneous and not periodic because of the use of IP Multicast to send the link-state updates. Updates are only sent when routing changes occur instead of periodically, ensuring better use of available bandwidth.

OSPF employs "flooding" to exchange link-states with other routers. Any change in routing information is flooded to all routers in the network. The use of "areas" puts a boundary on the explosion of link-state updates. All routers within an area will have the exact link-state database.

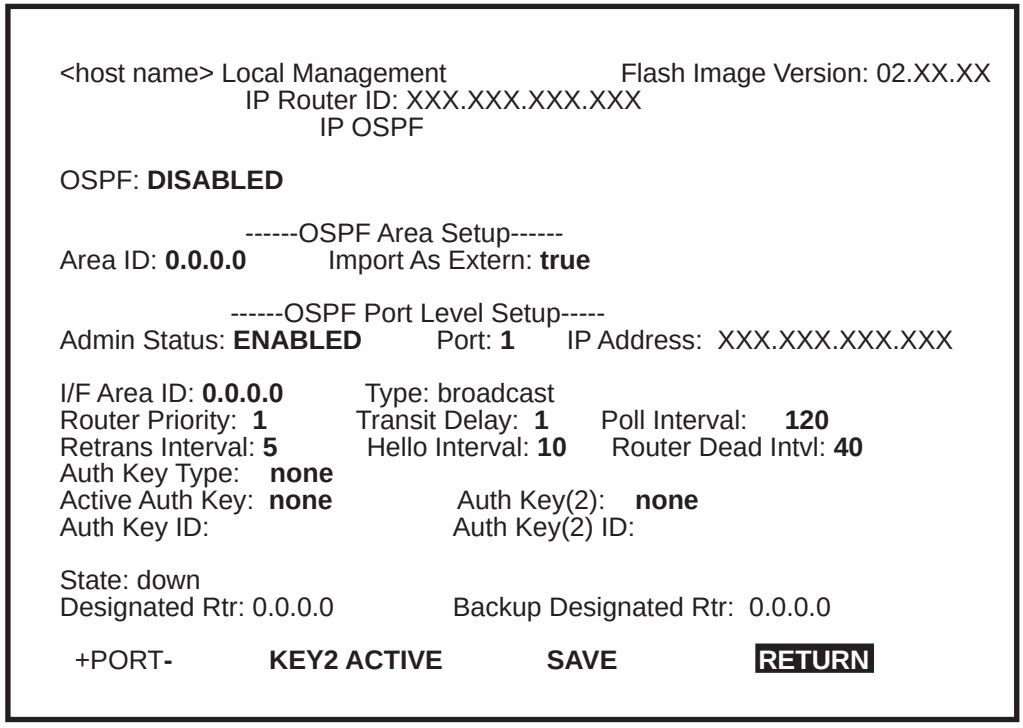

<host name> Local Management Flash Image Version: 02.XX.XX
IP Router ID: XXX.XXX.XXX.XXX
IP OSPF
OSPF: DISABLED
------OSPF Area Setup------
Area ID: 0.0.0.0 Import As Extern: true
------OSPF Port Level Setup-----
Admin Status: ENABLED Port: 1 IP Address: XXX.XXX.XXX.XXX
I/F Area ID: 0.0.0.0 Type: broadcast
Router Priority: 1 Transit Delay: 1 Poll Interval: 120
Retrans Interval: 5 Hello Interval: 10 Router Dead Intvl: 40
Auth Key Type: none
Active Auth Key: none Auth Key(2): none
Auth Key ID: Auth Key(2) ID:
State: down
Designated Rtr: 0.0.0.0 Backup Designated Rtr: 0.0.0.0
+PORT- KEY2 ACTIVE SAVE RETURN
ipospf

Figure 1-16 IP OSPF Configuration Screen

To enable OSPF complete the following steps:

1. From the Router Select screen, select **IP** and press ENTER. The IP Configuration screen displays.
2. From the IP Configuration screen, use the arrow keys to select **IP OSPF**. Press ENTER, and the IP OSPF Configuration screen shown in **Figure 1-16**, displays.
3. Use the arrow keys to select **OSPF: Disabled**. Press ENTER. The selection will toggle to **Enabled**.
4. Use the arrow keys to select **Area ID: 0.0.0.0**. Enter the Area ID number in dotted decimal format (000.000.000.000). When you have finished entering the area ID number, use the arrow keys to select **Admin Status:**. If Admin Status is Disabled, press ENTER to toggle the status to **Enabled**. Use the arrow keys to select **Port:**. Type the port number you wish to use. Press ENTER, and the port will be changed to the number that you typed.

5. Use the arrow keys to select **I/F Area ID**. Enter the I/F Area ID in dotted decimal notation (000.000.000.000). When you have finished, use the arrow keys to select **Router Priority**.

6. Type in the number representing the router priority you desire. When you have finished, use the arrow keys to select **Retrans Interval**. Enter the number of seconds of delay between retransmission of link-state advertisements. When you have finished, use the arrow keys to select **Transmit Delay**.

7. Type the number of seconds you wish to set for transmit delay. Transmit delay represents the estimated number of seconds it takes to transmit a link-state update packet over this interface. Link-state advertisements contained in the Link-state update packet will have their age incremented by this amount before transmission. This value must take into account transmission and propagation delays. When you have finished, use the arrow keys to select **Hello Interval**.

8. Type the number of seconds that you wish to use for the Hello Interval. The Hello Interval is the length of time in seconds between Hello packets that the router sends on this interface, advertised in Hello packets sent out of this interface. When you have finished use the arrow keys to select **Poll Interval**.

9. Type the number of seconds that you wish to use for Poll Interval. If a neighboring router has become inactive (Hello packets have not been sent for [router dead] seconds, it may be necessary to send Hello packets to the dead neighbor. The packets will be sent at a reduced rate [Poll Interval}, which should be much larger than the Hello Interval. A typical Poll Interval for an X.25 network is 120 seconds. When you have finished, use the arrow keys to select **Router Dead Interval**.

10. Type the number of seconds that you wish to use for Router Dead Interval. Router Dead Interval is the number of seconds before the router's neighbors will declare it down, when they stop hearing the router's Hello packets. When you have finished entering the Router Dead Interval, use the arrow keys to select **SAVE**. Press ENTER. The event message field at the top of the screen displays "SAVED OK".

IPX Configuration Screen

The IPX Configuration screen enables you to access the IPX General Config, IPX RIP, and IPX SAP screens to configure the HSIM or CyberSWITCH for IPX Routing and enable RIP routing or Source Advertisement Protocol (SAP) routing on the HSIM or CyberSWITCH.

Access the IPX Configuration screen, shown in **Figure 1-17**, by using the arrow keys to highlight the **IPX** menu item on the Router Setup and pressing ENTER. The IPX Configuration screen displays.

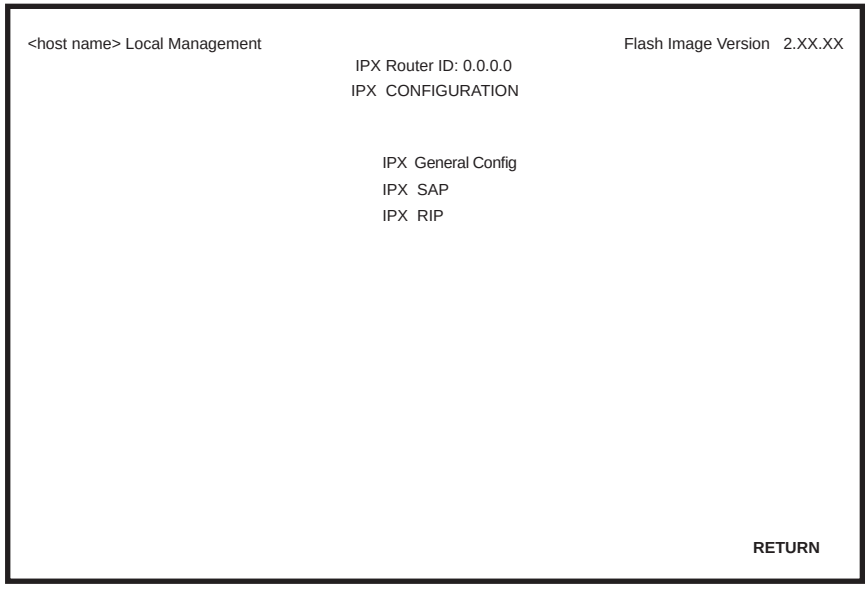


Figure 1-17 IPX Configuration Screen

IPX Configuration Fields

The following list describes each of the IPX Configuration screen fields.

IPX General Config — Use this field to access the IPX General Config screen and configure the HSIM or CyberSWITCH for IP routing.

IPX SAP — Use this field to access the IPX SAP screen and enable Source Advertisement Protocol (SAP) routing.

IPX RIP — Use this field to access the IPX RIP screen and enable the Routing Information Protocol (RIP).

IPX General Configuration Screen

The IPX General Configuration screen allows you to configure the HSIM or CyberSWITCH for IPX routing.

To access the IPX General Configuration screen, use the arrow keys to highlight the **IPX General Config** menu item and press ENTER. The IPX General Configuration screen shown in **Figure 1-18** displays.

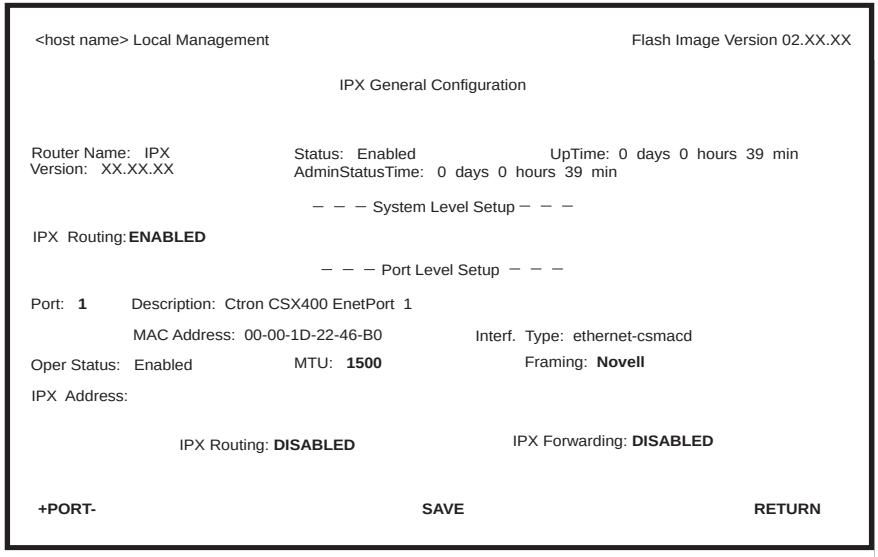


Figure 1-18 IPX General Configuration Screen

IPX General Configuration Status Fields

The following list describes each of the IPX General Config status fields. The status fields are for informational purposes only and cannot be modified.

Router Name — Displays the type of routing used.

Status — Displays the status of IPX Routing.

UpTime — Displays the amount of time elapsed since the last time the HSIM or CyberSWITCH was rebooted.

Version — The version number of the IP Routing used on the HSIM or CyberSWITCH.

AdminStatusTime — Displays the amount of time elapsed since an IP address was assigned to the HSIM or CyberSWITCH.

Description — Describes the selected Port.

MAC Address — Displays the physical (MAC) address of the HSIM or CyberSWITCH.

Interf. Type — Displays the type of interface used by the specified port.

Oper Status — Displays the operational status of the selected port.

IPX General Configuration Fields

This section provides a general overview of the procedures required to configure the HSIM or CyberSWITCH. The following list describes each of the IPX General Config fields.

+PORT- — Use this field to select the routing port that you wish to configure.

Framing — Use this field to select the format of the Frame in which IPX packets are encapsulated for transmission.

MTU — Use this field to set the Maximum Transmission Unit (MTU).

IPX Routing — Use this field to enable IPX Routing Services.

IPX Forwarding — Use this field to enable IPX Forwarding.

IPX Address — Use this field to assign an IPX Address to the port that you wish to configure.

Selecting a Port for Configuration

Routing Services allows you to choose the ports that you want to configure for IPX routing. To select a router port to configure for IPX routing, complete the following steps:

1. Use the arrow keys to highlight the **PORT** option.
2. Type in the number of the port that you want to configure for IPX routing, then press ENTER.

You can type in the port number, or you can use the +**PORT**- option at the bottom of the screen to scroll through the list of the ports on your device. To use the +**PORT**- option, use the arrow keys to highlight the + (to go forward), or the - (to go backward), and then press **ENTER** to scroll through the available ports in the direction you have selected. You can also use the **+** and **-** keys to scroll through the available ports.

If you type in an invalid port number the error message: “PORT NUMBER IS OUT OF RANGE” displays. Perform steps 1 and 2 again.

Entering the IPX Address

All IPX hosts must have an IPX Address for each network interface. These addresses identify each network connection.

To enter the IPX Address for a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX ADDRESS** option.
2. Type in the IPX Address in Dotted Decimal Notation (DDN) format and then press ENTER.

Selecting the Frame Type for a Port

On each port, Frame Type specifies the format of the frame in which IPX packets are encapsulated for transmission. The Frame Type options available for each router port are dependent on the type of media supported by that router port. Select the Frame Type based on your implementation, such as Encap-enet for bridging and Native-wan for routing. The choices are: Ethernet, SNAP, i8022,Slip, Novell, Localtalk, Native-wan, Encap-enet, Encap-enet-8022, Encap-enet-snap, Encap-enet-novell, Encap-tokenring-8022, Encap-tokenring-snap, Encap-fddi-8022, Encap-fddi-snap, Other.

To select the Frame Type for a port, complete the following steps:

1. Use the arrow keys to highlight the **Framing** option.
2. Use the ENTER key to toggle the entry to the correct Frame Type for the port.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Setting the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit specifies the maximum packet size for all IPX packets that are transmitted.

To select the MTU for a port, complete the following steps:

1. Use the arrow keys to highlight the **MTU** option under Port Level Setup.
2. Enter an MTU value for the media used.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Enabling IPX Routing Services on a Port

The ability to switch IPX Routing Services on and off on a port-by-port basis provides great flexibility. On the same device, some ports can be routing IPX traffic while other ports are bridging it. As you are in transition from a bridged network to a routed network, this flexibility allows you to implement IPX routing and test your routing configuration on a port-by-port basis. If necessary, you can temporarily disable IPX routing on any port without losing your configuration, or you can temporarily switch from IPX routing back to bridging.

To enable IPX Routing Services on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX Routing** option under Port Level Setup.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Enabling IPX Forwarding on a Port

By default, IPX Forwarding is disabled on each router port. Your device cannot begin forwarding IPX data packets on any router port until you enable IPX Forwarding on that port.

To enable IPX Forwarding on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX Forwarding** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

IPX Routing over Frame Relay

An additional step is required when routing IPX over Frame Relay. This step requires that entries are created in the IPX Host Map. The IPX Host Map is a database of remote IPX hosts that are defined generally by the WAN Network number and MAC Address, and more specifically by the Interface Number and Data Link Connection Identifier (DLCI). The IPX Host Map helps a routing decision by determining which circuit a packet should be forwarded to in a point to multi-point Frame Relay connection.

Figure 1-19 shows how IPX Host Map entries are entered using the circuitmap command. The circuitmap command is accessed from the **MIB Navigator Screen**. Refer to **Chapter 2** for more information on the circuitmap command.

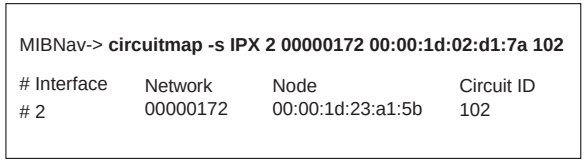


Figure 1-19 Circuitmap Command

The circuitmap command contains the following fields:

 # Interface — An entry must be created for each remote Router connected via the Frame Relay interface.

Network — The Network is the IPX Network number associated with the Frame Relay network.

Node — The Node is the MAC address of the remote router on the other end of the WAN link.

Circuit ID — The Circuit ID is the DLCI identifying the virtual circuit connection to the Telco.

Enabling the IPX SAP Routing Protocol on a Port

IPX Source Advertisement Protocol (SAP) is used by IPX to exchange information about Novell service providing nodes, such as file servers and print servers that are available. IPX SAP builds and maintains a database, the Service Advertisement Table, containing the addresses and routes to specific service providing nodes, and advertises this information over the network.

Each router running IPX SAP gathers this LAN based information from the locally connected network segments and adds it to its Service Advertisement Table. Each table contains the Novell Network Number and type of services available on all Novell servers known to the IPX SAP. IPX routing services uses this information to provide internetworked NetWare clients with access to these services.

To enable SAP Routing, complete the following steps:

1. From the IPX Configuration screen, highlight **IPX SAP** and then press ENTER.

   The IPX SAP Configuration screen, shown in **Figure 1-20**, displays.

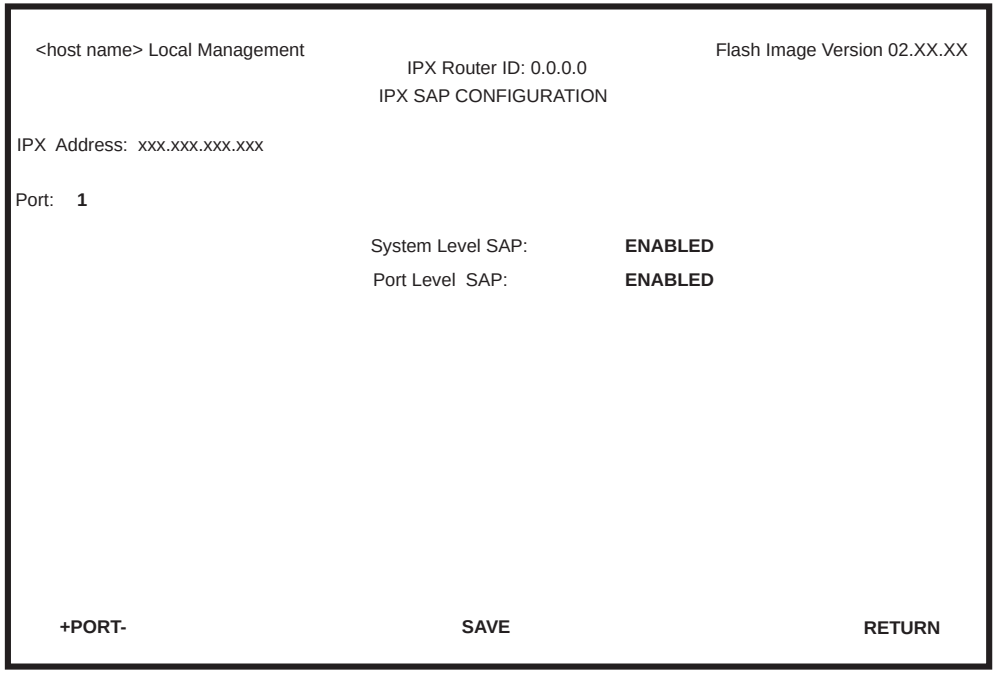


Figure 1-20 IPX SAP Configuration Screen

2. Use the arrow keys to highlight the **Port** option.
3. Type in the number of the port that you wish to enable SAP routing, then press ENTER.
4. Use the arrow keys to highlight the **Port Level SAP** option.
5. Use the ENTER key to toggle the entry to **ENABLED**. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message "SAVED OK" displays.

Enabling RIP on a Port

IPX RIP (Routing Information Protocol) is a widely implemented routing protocol that is used extensively on IPX intermediations. IPX Routing Services uses the RIP to send and gather information about the internetwork topology. This information is used to construct and maintain a database, called the RIP Route Table, containing the addresses and available routes to all the networks and hosts that RIP has learned.

Enabling RIP allows IPX Routing Services to build and maintain a dynamic database of route information. The best routes learned by RIP are added to the IPX Forwarding Table to be used to forward IPX packets. The ability to switch RIP on and off on a port-by-port basis provides great flexibility. On the same device, some router ports can be running RIP while other router ports are not. If necessary, you can temporarily disable RIP on any port without affecting the rest of your configuration.

To enable RIP Routing, complete the following steps:

1. From the IPX Configuration screen, highlight **IPX RIP** and then press ENTER. The IPX RIP Configuration screen, shown in **Figure 1-21**, displays.

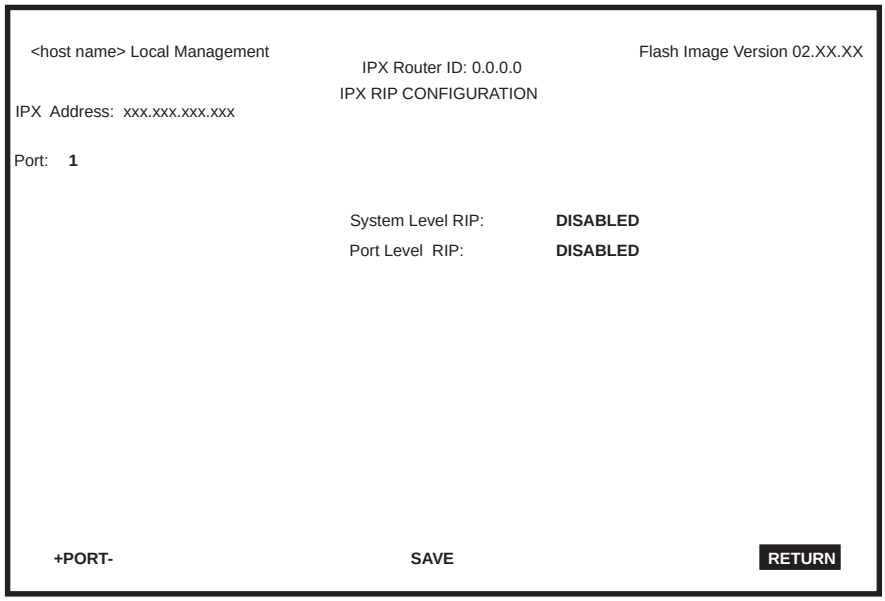


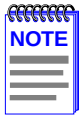
Figure 1-21 IPX RIP Configuration Screen

2. Use the arrow keys to highlight the **Port** option.
3. Type in the number of the port that you wish to enable RIP routing and then press ENTER.
4. Use the arrow keys to highlight the **Port Level RIP** option.
5. Use the ENTER key to toggle the entry to **ENABLED**. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message "SAVED OK" displays.

2 WAN CONFIGURATION

This chapter explains how to configure the HSIM or CyberSWITCH through Local Management for WAN service. The WAN Setup menu item accesses screens which allow you to configure the HSIM or CyberSWITCH for a WAN Physical Interface Module (WPIM).

Refer to the host platform User's Guide for instructions about how to set up and access Local Management.



Refer to the Cabletron Systems *HSIM-SSA710 User's Guide* for information on the HSIM-SSA710.

Chapter Organization

The following list shows the organization of this chapter:

- The WAN Physical Configuration screen
- WPIM Timeslot Configuration Table
- The WAN Interface Configuration screen
- Remote Profiles Setup
- Bandwidth-on-Demand (Multilink Protocol) Configuration
- T1 Configuration
- Frame Relay Configuration
- DDS Configuration
- Troubleshooting the Frame Relay Connection
- Call Backup Configuration

The WAN Physical Configuration Screen

To access the WAN Physical Configuration screen, use the arrow keys to highlight the **WAN SETUP** menu item, then press ENTER. The screen shown in **Figure 2-1** displays.

When there is more than one WPIM installed into the host platform, information for the second WPIM will display next to WPIM 1.

The HSIM or CyberSWITCH supports a variety of WPIMs with the exception of the HSIM-W84 which always employs four T1 WPIMs. **Figure 2-1** shows the WAN Physical Configuration screen for a device containing a WPIM-HDSL and a WPIM-T1. To select the WPIM you wish to configure, use the arrow keys to highlight the [WPIM #] field at the bottom of the screen. Use the SPACE bar to select the appropriate WPIM, then press ENTER.

```
Local Management                              Flash Image Version: 02.00

                        WAN PHYSICAL CONFIGURATION

      WPIM 1                 WPIM 2
Type:   T1             Type:   HDSL
WPIM #  1              WPIM #  2
MgrType:[ISDN BRI]     MgrType:[NONE]
Max VCs:016            Max VCs:000
Next IF:003            Next IF:N/A


  WPIM 2 Line Configuration

HDSL Tx Clock Source:                  [Loop-Timing]
HDSL Loop-Back:                        [None]
HDSL Timeslot Configuration:           [Fractional]




   SAVE    [WPIM 2]    WAN INT CONFIG    REMOTE SETUP    RETURN
```

Figure 2-1 WAN Physical Configuration Screen

WAN Physical Configuration Screen Fields

The following sections describe WAN Physical Configuration screen fields and provide instructions for setting them. The WAN Physical Configuration screen lets you configure the WPIM or "Physical Interface."

To select the WPIM you wish to configure, proceed as follows:

1. Use the arrow keys to highlight the **WPIM X** command field at the bottom of the screen.
2. Use the SPACE bar to select the appropriate WPIM, then press ENTER. The WAN Configuration screen automatically displays unique configuration fields for each WPIM as shown in **Figure 2-1**.

The WAN Physical Configuration screen displays the following information for each WPIM:

WPIM *1-2* (Read-Only) — Displays configuration information for up to two different WPIMs.

Type (Read-Only) — Displays the type of WPIM installed in the slot.

WPIM # (Read-Only) — Displays the number of the slot in which the WPIM resides.

Mgr Type (Selectable) — Used to select the type of protocol manager. The available options are PPP, FR PtoMP, FR PtoP, HDLC and NONE. The field defaults to NONE.

Max VCs (Modifiable) — Displays the maximum number of virtual circuits (interfaces) available to be configured. The default number displayed depends on the Protocol Manager chosen. The MAX VC value associated with a physical WAN interface is set to a default value based on the number of possible ports available and the protocol manager selected. If, in the case of Frame Relay or ISDN BRI, more PVCs/DLCIs exist than the default MAX VC value will allow, the MAX VCs may be changed.

Next IF (Read-Only) — Displays the next interface available to be used.

Command Fields:

SAVE (Command) — Saves the chosen configuration.

[WPIM X] (Toggle) — Enables the user to select the WPIM to be configured. Once it is selected, the user can enter the screens of the WPIM selected to modify the data.

WAN INT CONFIG (Command) **—** When this field is highlighted and the ENTER key is pressed, the WAN Interface Configuration screen displays. Refer to the **WAN Interface Configuration Screen** section.

REMOTE SETUP (Command) **—** Used to access and modify remote profiles information.

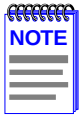
RETURN (Command) **—** Returns user to the previous screen in the hierarchy.

HDSL Line Configuration Fields

HDSL Tx Clock Source — Displays the HDSL Transmit Clock Source. The selections for this field toggle between Loop-Timing (Extracted Line Data) and Local-Timing (Internal Clock). The default setting for this field is **Loop-Timing**.

HDSL Loopback — This is set to test the local loop for error conditions for the WPIM-HDSL. The available options are: NLOC, NREM, CLOC, CREM, CDU1, CDU2, NDU1, NDU2, and None. The field defaults to **None**.

For more information, see the Cabletron Enterprise WAN MIB ctwan-mib.txt for the HDSL loopback option information



The Loop-Timing selection in this Local Management screen corresponds to the Slave selection in the QuickSET HDSL WAN Configuration window; the Local-Timing selection corresponds to the Master selection.

HDSL Timeslot Configuration — Displays the timeslot configuration for the WPIM-HDSL. The selections for this field toggle between Full and Fractional. The default setting for this field is **Full**. Full uses all 24 timeslots and Fractional uses the first 12 timeslots.

T1 Line Configuration Fields

The configuration fields displayed on the WAN Physical Configuration screen shown in **Figure 2-3** are specific to the T1 mode of the HSIM or CyberSWITCH.

The service provider (i.e., AT&T, Sprint, MCI, Bell Atlantic, etc.) determines the settings for the following fields. Consult the service provider for the correct settings.

T1 Timeslot View (Toggle) **—** Displays the status of the Timeslot Configuration Table. This field toggles between Active and New. The field comes up with the default setting **Active**. The Active setting displays current Timeslot Configuration table settings. The New setting allows you to change Timeslot Configuration table settings. The default setting for the Timeslot Configuration table is all timeslots not assigned (**000**).

T1 Line Coding (Toggle) **—** Displays the line coding for the physical T1 line. This field toggles between B8ZS and AMI. The default setting is **B8ZS**.

T1 Frame Type (Toggle) **—** Displays the T1 Frame type. This field toggles between ESF and D4. The default setting is **ESF**.

T1 Tx Clock Source (Toggle) **—** Displays the T1 Transmit Clock Source. This field toggles between Loop-Timing (Extracted Line Data) and Local-Timing (Internal Clock). The default setting is **Loop-Timing**.

T1 Line Buildout (Selectable) **—** Displays the line coding for the physical T1 line. Set this to 0 dB unless the service provider recommends another setting. The default setting for this field is **0 dB**. The following settings are available in this field:

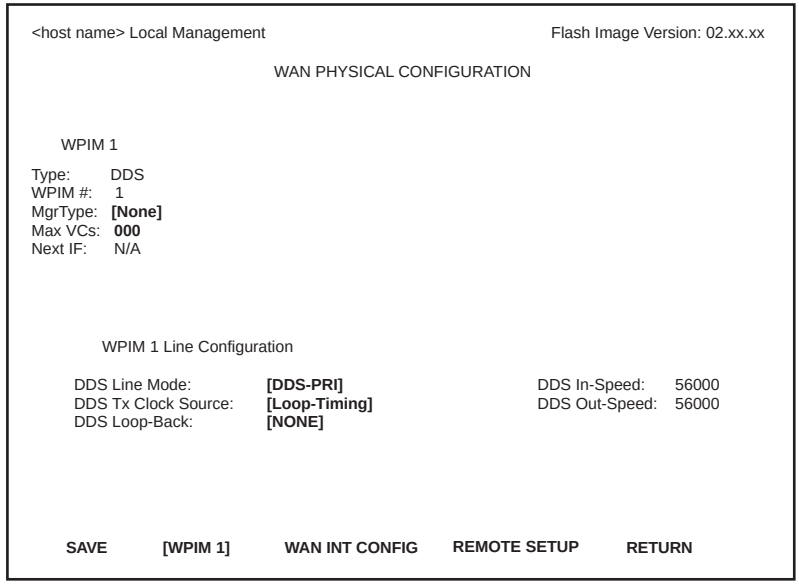
- 0 dB
- -7.5 dB
- -15 dB
- -22.5 dB
- 133-266 Ft
- 267-399 Ft
- 400-533 Ft
- 534-655 Ft

T1 Loopback (Selectable) **—** Network Loopback is a testing procedure that segments the line and allows the user to isolate faults. The selections for this field are None, Line-Loop, and Payload-Loop. In Line-Loop the entire T-1 line is looped back, including the framing bits, CRC, and the facility data link. This happens before the framer. In Payload-Loop, only the 24 time slots are looped back, which happens behind the framer, and does not include the framing bits, CRC, and facility data link. The HSIM or CyberSWITCH must be in Loop-Timing mode to use this option. The default setting is **None**.

Timeslot Configuration Table **—** The Timeslot Configuration Table (WPIM-T1 for the HSIM-W84) lets you configure the way in which the T1 time slots are used. The Configuration Table contains 24 time slots. You must assign each time slot an Interface Number. Time slots not used will be assigned a value of 000. If you lease an entire T1 line you can use all 24 time slots (the full T1 bandwidth). In the case of the HSIM-W84, available interfaces for T1-1 are 002 through 025, T1-2 are 026 through 049, T1-3 are 050 through 073, and T1-4 are 074 through 097.

DDS Line Configuration Fields

The configuration fields displayed on the WAN Physical Configuration screen shown in **Figure 2-2** are specific to the DDS mode of the HSIM or CyberSWITCH.



2750_01

Figure 2-2 WAN Physical Configuration Screen for DDS Service

DDS Line Mode (Toggle) **—** Displays the DDS Line Mode. The selections toggle between DDS-PRI (primary) and DDS-CC (clear channel). This field should be set according to information from the service provider. The default setting for this field is **DDS-PRI**.

DDS Tx Clock Source (Toggle) **—** Displays the clock source as either Loop-Timing or Local-Timing. The Loop-Timing setting allows the HSIM or CyberSWITCH to receive its timing information from the service provider, and the Local-Timing setting allows the HSIM or CyberSWITCH to receive its timing information internally. If DDS-CC is chosen for the DDS Line Mode then this field must be set to Loop. The default setting is **Loop**.

DDS Loop-back (Toggle) **—** Displays the internal Loopback as either Line-Loop or None. Line loopback is reserved for network diagnostics only. The default is **None**.

DDS In-Speed (Read-Only) **—** Displays 56000 (bps) for Primary DDS Line Mode and 64000 (bps) for Clear Channel DDS Line Mode upon start-up.

DDS Out-Speed (Read-Only) **—** Displays 56000 (bps) for Primary DDS Line Mode and 64000 (bps) for Clear Channel DDS Line Mode upon start-up.

WPIM Timeslot Configuration Table

The WPIM Timeslot Configuration table allows the user to configure the way in which the Cabletron Systems WAN module uses the T1 line. The configuration table consists of 24 timeslots. Each timeslot must be assigned an **Interface** number (for example, 002 for an active Interface number or 000 if the timeslot is not used). When an entire T1 line is leased, all 24 timeslots (the full T1 bandwidth) can be used. If only a fraction of the T1 line is leased, the service provider indicates which timeslots to use.

Figure 2-3 displays the T1 Line Configuration with the Timeslot View.

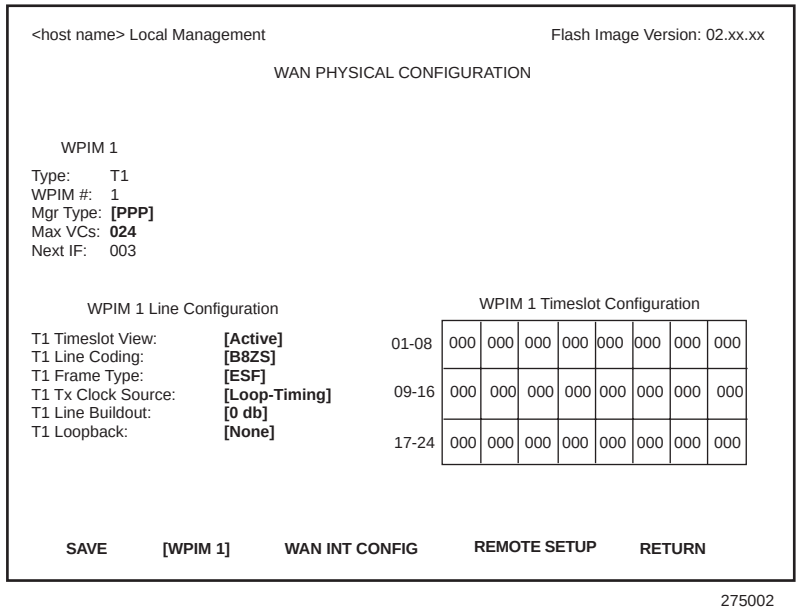


Figure 2-3 T1 Line Configuration showing Timeslot

Timeslots can be utilized in any way chosen. The HSIM or CyberSWITCH supports Time Division Multiplexing (TDM) allowing demultiplexing of circuits (timeslots) within the public network. For example, if the HSIM or CyberSWITCH has access to a full T1 (24 timeslots), and the user wants to communicate with two other sites, the configuration might look like the one shown in **Figure 2-4**.

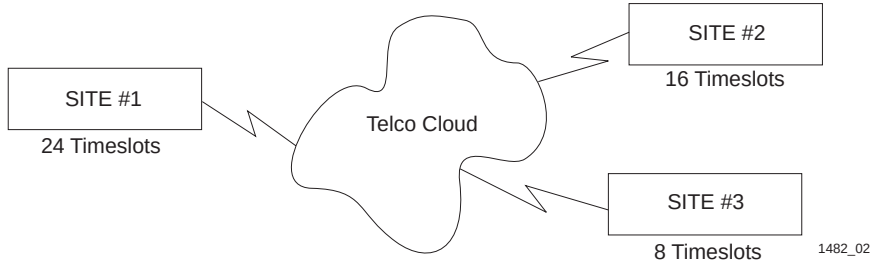


Figure 2-4 Sample Timeslot Configuration

Figure 2-5 shows a sample configuration for three sites. Of the 24 timeslots, Site #1 uses 16 to communicate with Site #2 and the remaining 8 to communicate with Site #3. This configuration varies tremendously depending on how the service provider maps out the T1 timeslots. The service provider indicates which timeslots are active.

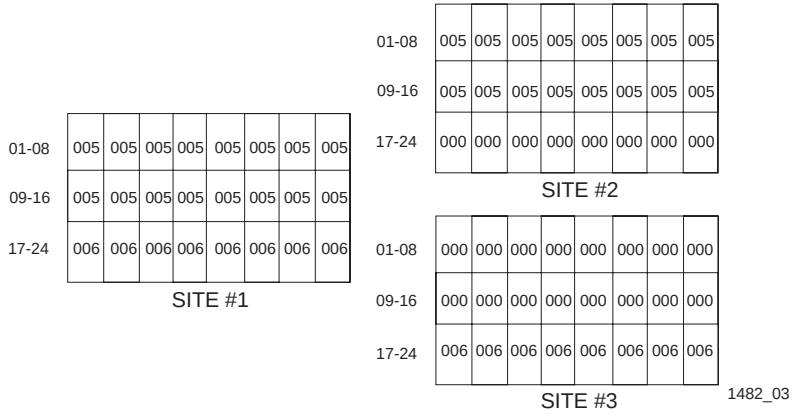
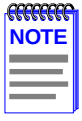


Figure 2-5 Sample Configuration

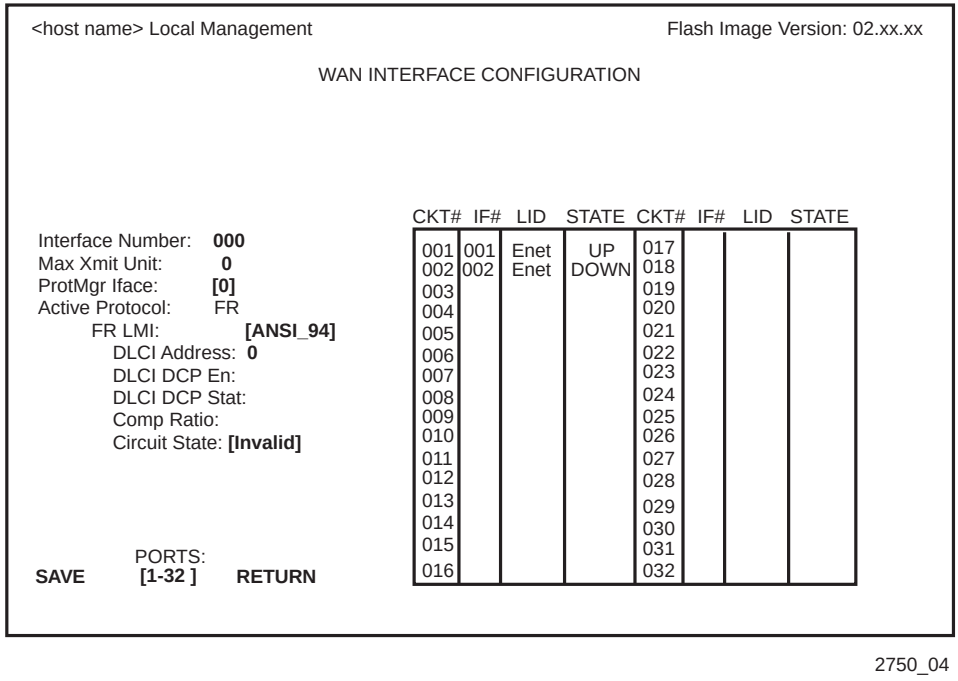
Site #1 is using the full T1, so all the timeslots must have an Interface assignment. Site #2 and Site #3 use only a fraction of the T1, but the total quantity of timeslots must match those of Site #1. Unused timeslots receive an Interface number of 000.



The Interface numbers of Site #1, Site #2 and Site #3 do not have to match. Only the **quantity** and **position** of timeslots must match (the service provider assigns the timeslots).

WAN Interface Configuration Screen

This section describes the features of the WAN Interface Configuration screen. Access the screen by using the arrow keys to highlight the **WAN INT CONFIG** command field at the bottom of the WAN Physical Configuration screen, then press ENTER. The WAN Interface Configuration screen displays, as shown in **Figure 2-6**.



2750_04

Figure 2-6 WAN Interface Configuration Screen

WAN Interface Configuration Screen Fields

This section describes the WAN Interface Configuration screen fields.

Interface Number (Modifiable) **—** Displays the active Interface Number. Use this field to configure the Interface Numbers assigned on the WAN Physical Configuration screen.

Max Xmit Unit (Modifiable) **—** User-configured field that displays the maximum packet size that can be transmitted on the selected Interface. Defaults are **1506** for PPP and **4095** for Frame Relay. The default settings for this field depend on the Protocol Manager chosen.

ProtMgrIface (Selectable) — Protocol Manager assigned for the interface number displayed. In the case of Frame Relay the Protocol Manager assigned to the FR link is automatically selected. This allows for mapping FR DLCI(s) when the interface number field has a 000 typed into it. Type the DLCI address into the DLCI address field. Press the SPACE bar to display “Inactive” in the Circuit State field, and then SAVE these changes.

Active Protocol (Read-Only) — Displays the active OSI layer protocol (Protocol Manager) chosen for the HSIM or CyberSWITCH. There is one set of parameters displayed for FR, and one set for PPP. Refer to the section titled **Frame Relay as the Protocol Manager** for information on the Active Protocol set to Frame Relay, and the section titled **PPP as the Protocol Manager** for PPP information.

Command and Interface Table Fields

SAVE (Command) — Saves the configuration changes.

PORTS: [1-32], [33-64], [65-96], [97-128] (Command) — Interface table displays the range of circuits shown in the command field. Use the SPACE bar and either the BACKSPACE or DELETE key to step through the displays.

RETURN (Command) — Returns user to the previous screen.

CKT# (Read-Only) — Displays the circuit number of the application ports available from the host platform. If the active protocol is PPP or FR PtoP, only one application port per interface number (IF#) is assigned. If the active protocol is FR PtoMP, the available WAN ports from the host platform may be assigned, one per DLCI.

IF# (Read-Only) — Displays the MIB II Interface number that is associated with the application port (CKT#).

LID (Read-Only) — Displays the Link Identifier. If the active protocol is Frame Relay, the Data Link Connection Identifier is displayed. If the active protocol for this interface is PPP, then PPP displays in this field. For Ethernet ports, Enet is displayed.

STATE (Read-Only) — Displays the status of the application port. If the active protocol is Frame Relay, this field displays the status as Active, Inactive, or Invalid (no LMI). If the active protocol is PPP or Ethernet, this field displays the Link Control Protocol (LCP) state, either UP (active) or DOWN (inactive). See PPP or FR commands within the MIB Navigator for more information on link status.

Frame Relay as the Protocol Manager

Refer to **Figure 2-3** for the following parameters displayed for FR.

In FR PToMP mode, DLCI's can be learned dynamically and do not need to be entered in the screen. Once a DLCI is entered, it becomes a "statically" entered DLCI. To remove a statically-entered DLCI, enter the IF# of the DLCI (see the Interface Screen), then enter "Invalid" into the Circuit State field, and then SAVE the changes.

FR LMI (Selectable) — Frame Relay Link Management Interface. Selectable states are based on the applicable RFC selections. The applicable switch type is chosen based on the switch type used by the Service Provider. The choices are: No LMI, T1.617-D, Q.933-A, and ANSI_94. The NO LMI setting is for specialized applications in which no Frame Relay Link Management is available or required.

DLCI Address (Modifiable) — Data Link Connection Identifier given by the Service Provider. It is the PVC mapped index number of the connection identifier. The Telco switch assigns a virtual port to each DLCI. Can be set to values from 0-1023, depending on the protocol, when available for modification with certain protocol modes. The values 0-15 and 1008-1022 are reserved DLCI addresses. When using FR PtoMP as the Protocol Manager, the HSIM or CyberSWITCH can learn the DLCIs dynamically from the switch.

DLCI DCP En (Toggle) — The Data Compression Protocol (DCP) can be enabled or disabled in this field, on an application port per application port basis, when available. The DLCI port must be entered to change compression. Use the SPACE bar to toggle the field and ENTER to select either On or Off.

DLCI DCP Stat (Read-Only) — Displays the current negotiated status of compression.

Comp Ratio (Read-Only) — Displays the Compression Ratio, which is the ratio of uncompressed to compressed data.

Circuit State (Selectable) — The field initially displays the state of the DLCI circuit, and can be modified. Steps through Active, Inactive and Invalid.

PPP as the Protocol Manager

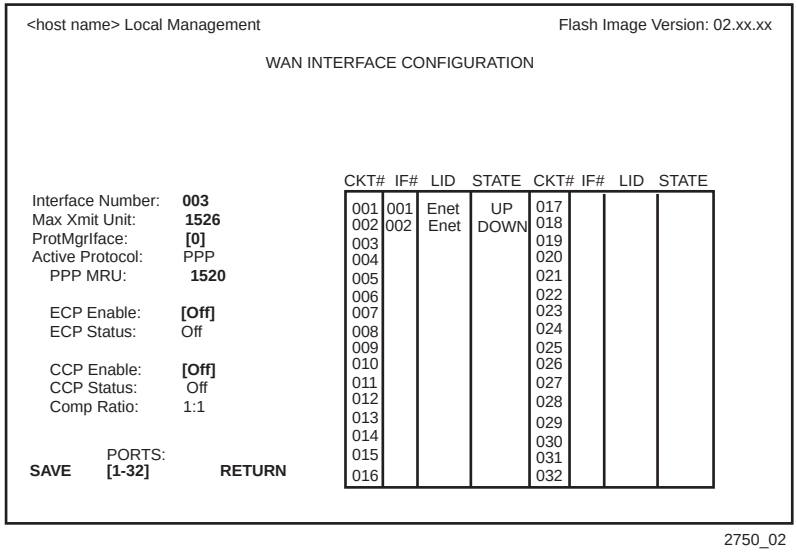


Figure 2-7 WAN Interface Configuration Screen (PPP)

Refer to **Figure 2-7** for the following parameters displayed for PPP.

PPP MRU (Modifiable) — Displays the modifiable Maximum Receive Units that PPP can handle.

ECP Enable (Toggle) — Toggles between On and Off to enable or disable encryption.

ECP Status (Read-Only) — Displays the status of encryption.

CCP Enable (Toggle) — Toggles between On and Off to enable or disable compression.

CCP Status (Read-Only) — Displays the status of compression.

Comp Ratio (Read-Only) — Displays the Compression Ratio, which is the ratio of uncompressed to compressed data.

Remote Profiles Setup

To access the Remote Profiles Setup screen from the WAN Physical Configuration screen, use the arrow keys to highlight the **Remote Setup** option, then press ENTER. The screen shown in **Figure 2-8** displays.

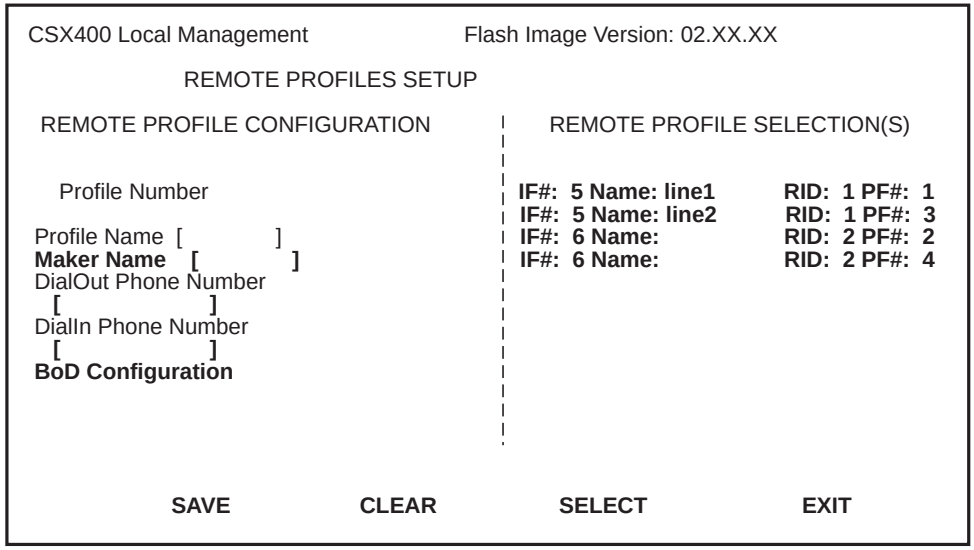


Figure 2-8 Remote Profiles Setup Screen

Remote Profiles Setup Screen Fields

The following section describes the Remote Profiles Setup screen fields and instructions for navigating in the Remote Profiles table.

Once in the Remote Profiles Setup screen, use the arrow keys to navigate to and highlight the **SELECT** option. Press ENTER to allow navigation in the Remote Profiles Selection(s) area of the screen. Choose the profile that is to be modified using the arrow keys and press ENTER once it is highlighted.

The fields in the Remote Profiles Selection(s) are defined as follows:

IF# — Interface number of the profile.

Name — The name of the profile as defined by the user.

RID — Remote Identifier.

PF # — Profile number, the information used to describe a possible connection.

Once the desired profile is selected, the following fields of the selected profile can be set or modified as desired: Profile Name, Maker Name, Calling Number, and Caller Number.

The BoD Configuration selection leads to a menu that allows you to set and configure Multilink Protocol (MP) support. This menu is described in the section titled **Bandwidth-on-Demand (Multilink Protocol) Configuration**.

The command fields at the bottom of the screen are defined as follows:

SAVE — Allows the user to save the configuration in NVRAM once changes have been made.

CLEAR — Allows the user to clear an entire profile.

SELECT — Allows the user to enter the Remote Profile Selection(s) area in order to choose the profile to configure or modify.

EXIT — Exits the current screen.

PREV/NEXT — The Remote Profile Selection(s) screen will not display more than 10 profiles at a time. When there are more than 10 profiles to be displayed, the choices PREV and NEXT will display at the bottom of the screen. Highlight NEXT to go to the screen after the currently displayed screen, and PREV to go to the screen before the currently displayed screen. There is a maximum of 20 profiles.

Bandwidth-on-Demand (Multilink Protocol) Configuration

To access the Bandwidth-on-Demand Configuration screen from the Remote Profiles Setup screen, use the arrow keys to highlight the **BoD Configuration** option, then press ENTER. The screen shown in **Figure 2-9** displays. The screen is laid out with the parameter name in the left column, the min-max settings in the second column, and the modifiable display field in the third column.

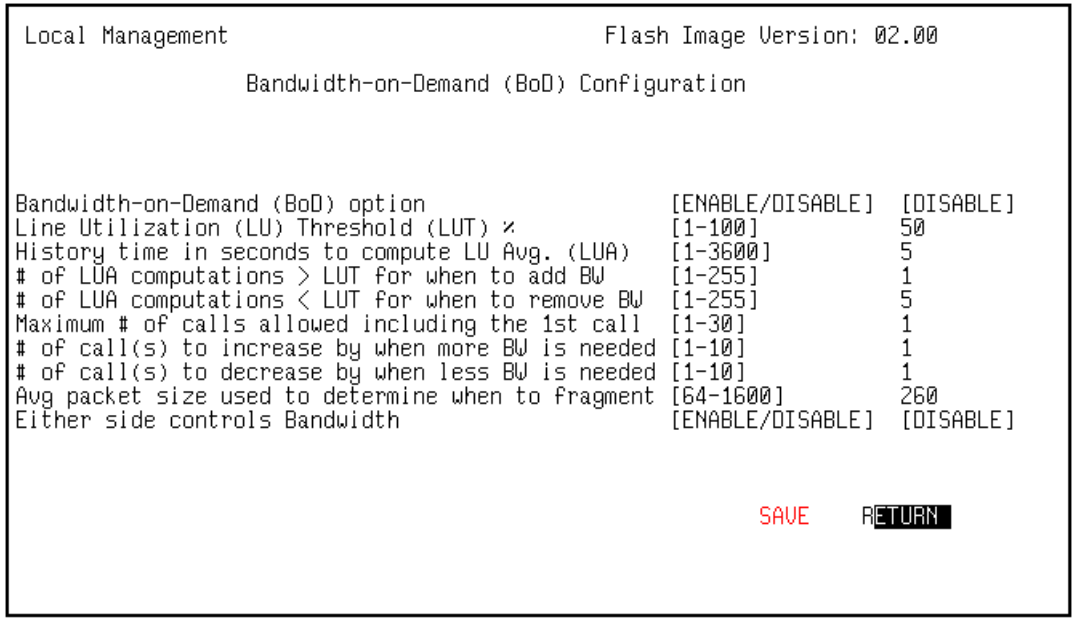

Local Management
Flash Image Version: 02.00
Bandwidth-on-Demand (BoD) Configuration
Bandwidth-on-Demand (BoD) option [ENABLE/DISABLE] [DISABLE]
Line Utilization (LU) Threshold (LUT) % [1-100] 50
History time in seconds to compute LU Avg. (LUA) [1-3600] 5
# of LUA computations > LUT for when to add BW [1-255] 1
# of LUA computations < LUT for when to remove BW [1-255] 5
Maximum # of calls allowed including the 1st call [1-30] 1
# of call(s) to increase by when more BW is needed [1-10] 1
# of call(s) to decrease by when less BW is needed [1-10] 1
Avg packet size used to determine when to fragment [64-1600] 260
Either side controls Bandwidth [ENABLE/DISABLE] [DISABLE]
SAVE
RETURN

Figure 2-9 Bandwidth-on-Demand Configuration Screen

The Bandwidth-on-Demand Configuration screen allows BoD parameters to be easily programmed and displayed. The display shows the minimum and maximum settings that the parameters can be set to, and the current value is displayed after the min-max settings.

Use the arrow keys to select and highlight the desired parameter to modify. The first and last parameters, “BoD option” and “Either side controls Bandwidth” option, are modified by using the SPACE bar to select the option desired once the field is highlighted. The default for these fields is **DISABLE**.

Use the numerical input keys to enter the desired number for all the numerical input fields when selected.

The fields for the BoD feature are described as follows:

Bandwidth-on-Demand (BoD) option — Specifies whether or not MP support is desired. To successfully negotiate MP, both devices must support MP. The default setting is **DISABLE**.

Line Utilization (LU) Threshold (LUT)% — Specifies a line utilization threshold (%) value to compare against the linear weighted percentage by which to determine when more or less bandwidth is to be added or removed. **The default setting is 50**.

History time in seconds to compute LU Avg. (LUA) — Specifies a time value in seconds over which the line utilization percentage is averaged by the linear weighted percentage algorithm. **The default setting is 5**.

# of LUA computation(s) > LUT for when to add BW — Specifies the number of samples for which the condition for adding more bandwidth must persist before additional bandwidth is added. This parameter is used to filter out traffic bursts. The value should be chosen such that the time it takes to add more bandwidth is less than the time the traffic will exceed the "line threshold". This will avoid the additional cost of adding unnecessary bandwidth. **The default setting is 1**.

# of LUA computation(s) < LUT for when to remove BW — Specifies the number of seconds that the output has fallen below the line threshold before possible previously added additional bandwidth is removed. **The default value is 5**.

Maximum # of calls allowed including the 1st call — Specifies the maximum number of channels an MP call is allowed. The value accounts for the channel used to establish the original/first link. **The default setting is 1**.

When modifying the "Maximum # of calls allowed" parameter, which accounts for the first call, a check is first made against the maximum profiles setting for that interface. Although the maximum possible value allowed is shown to be 20, the true maximum is the current maximum profiles setting for that interface (which cannot exceed 20).

# of calls to increase by — Specifies the incremental number of channels by which to increase additional bandwidth. Specifically, channels can be added in multiples. **The default setting is 1**.

# of calls to decrease by — Specifies the decremental number of channels by which to remove bandwidth. Specifically, channels can be removed in multiples. **The default setting is 1**.

Avg packet size used to determine when to fragment — Specifies the average packet size by which to determine when it is best to split a packet. This minimizes the amount of buffering necessary at the remote device to maintain packet sequentiality. **The default setting is 260**.

Either side controls Bandwidth — Specifies whether or not bandwidth changes are permitted by either side, i.e., both parties. Normally only the caller controls the bandwidth. The default setting is **DISABLE**.

Configuration: Full T1 Configuration Using PPP

This section provides step-by-step instructions for configuring the HSIM or CyberSWITCH to use a full T1 circuit in a PPP environment. This simplified example assumes the setup shown in **Figure 2-10** using a CSX400 with a HSIM or CyberSWITCH installed at Site #1. Configurations may vary depending on the host platform.

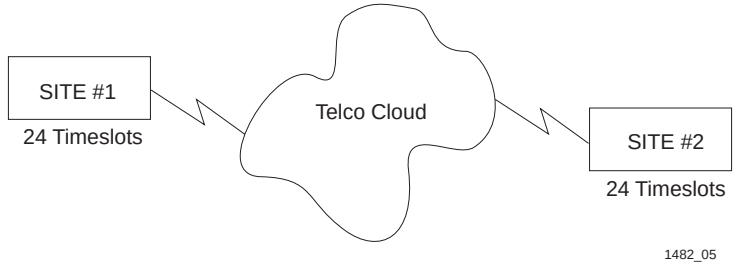


Figure 2-10 Full T1 Configuration

The line configuration information shown in **Table 2-1** must be supplied by the service provider.

Table 2-1 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
Line Coding	B8ZS or AMI
Frame Type	ESF or D4
Clock Source	Loop Timing or Local Timing

T1 Physical Configuration

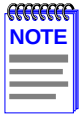
Begin the T1 configuration by accessing the WAN Physical Configuration screen through Local Management (**Figure 2-3**). Access the WAN Physical Configuration screen from the WAN SETUP menu item in the host platform.

Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM X]** field at the bottom of the screen. Press the SPACE bar to select the number of the WPIM to be configured, then press ENTER.
2. Use the arrow keys to highlight **MgrType**. Select PPP.

When changing from one protocol to another on a HSIM or CyberSWITCH that has been operational, save NONE as the protocol before changing to another protocol.

3. Use the arrow keys to highlight **Timeslot View**. Press the SPACE bar to select **New**, then press ENTER. The cursor moves to timeslot #1 of the Timeslot Configuration Table.
4. Insert an interface number into every timeslot as needed (refer to the note below). Type the number, press ENTER, then use the arrow keys to highlight the next timeslot field. Exit this field by using the arrow keys. The cursor automatically moves to the **T1 Line Coding** field.



The value assigned to the timeslots is the interface being used for WAN communication. The next available interface is displayed on the WAN Physical Configuration screen in the Next IF field (see **Figure 2-3**). The Next IF number shown must be used to add a new interface. The Next IF will increment as interfaces are added. The previously entered interfaces can be modified by entering the interface number.

The following four steps are based on information supplied by the service provider. Consult the service provider for the correct settings.

5. Use the arrow keys to highlight **T1 Line Coding**. Press the SPACE bar to select **B8ZS** or **AMI**, then press ENTER.
6. Use the arrow keys to highlight **T1 Frame Type**. Press the SPACE bar to select **ESF** or **D4**, then press ENTER.
7. Use the arrow keys to highlight **T1 TX Clock Source**. Press the SPACE bar to select **Local** (no clock source provided by telephone company) or **Loop** (clock source provided by telephone company), then press ENTER.

If you are using a Local clock source, set only one end of the circuit for Local, and the other end must be set for Loop.

8. Use the arrow keys to highlight **T1 Line Buildout** (LBO). Press the SPACE bar to select **0 dB** unless the service provider recommends another setting, then press ENTER.
9. Use the arrow keys to highlight **T1 Network Loopback.** Press the SPACE bar to select **None**, then press ENTER.
10. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "SAVE DONE!" displays and Local Management saves the changes to memory. "REBOOT IN PROGRESS....." displays and the host platform reboots. Re-entry to management is necessary for any further configuration.
11. Proceed to the next section to continue configuration.

T1 Interface Configuration

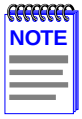
The WAN Interface Configuration screen is accessed through the WAN Physical Configuration screen. Access the WAN Interface Configuration screen by using the arrow keys to highlight the WAN INT CONFIG command and press ENTER. Refer to **Figure 2-6** and proceed with the following steps to configure the WAN Interface.

1. Set the WAN connection Interface Number by typing the same number into the **Interface Number** field that was input into the timeslots in the WAN Physical Configuration screen, then press ENTER (see the Note on **page 2-19**).
2. Unless the user sets the Max Xmit Unit, the HSIM or CyberSWITCH automatically sets the **Max Xmit Unit** to **1526** (default for PPP) after the protocol manager type is selected.
3. Make any changes to the available settings as desired.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory.

The WAN configuration is complete. It takes up to 60 seconds for the WAN Interface to come out of standby and for communications to begin.

Configuration: Fractional T1 Configuration Using PPP

This section provides step-by-step instructions for configuring the HSIM or CyberSWITCH to use a fractional T1 circuit in a PPP environment. This example assumes the setup shown in **Figure 2-11** using two CSX400s with each containing a HSIM or CyberSWITCH. Configurations may vary depending on the host platform. In a fractional T1 setup, only a portion of the 24 timeslots or DS-0s are used.



The terms DS-0 (Digital Signal, level 0) and timeslot are used synonymously in this guide to represent a standard 64,000 bps channel.

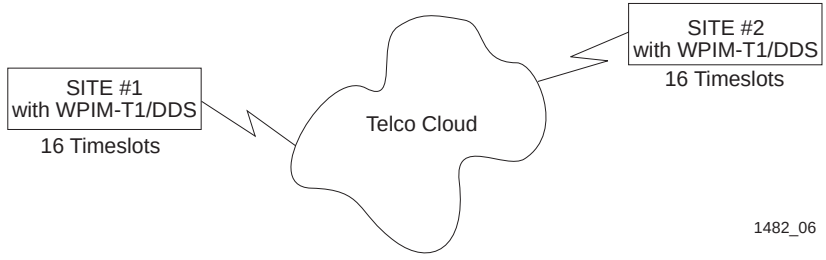


Figure 2-11 Fractional T1 Configuration

The line configuration information shown in **Table 2-2** must be supplied by the service provider.

Table 2-2 Telco Configuration Information

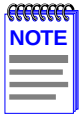
Configuration Information Required by User	Information Supplied by Service Provider
Line Coding	B8ZS or AMI
Frame Type	ESF or D4
Clock Source	Loop Timing or Local Timing
DS-0s (timeslots)	Timeslots being used for each end of the circuit

T1 Physical Configuration

Begin the HSIM or CyberSWITCH physical configuration by accessing the **WAN Physical Configuration** screen through Local Management (**Figure 2-1**).

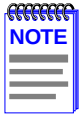
Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM X]** field at the bottom of the screen. Press the SPACE bar to select the number of the WPIM being configured, then press ENTER.
2. Use the arrow keys to highlight **MgrType**. Select PPP.



When changing from one protocol to another on a HSIM or CyberSWITCH that has been operational, save NONE as the protocol before changing to another protocol.

3. Use the arrow keys to highlight **Timeslot View**. Press the SPACE bar to select **New**, then press ENTER. The cursor moves to Timeslot #1 of the Timeslot Configuration Table.
4. Insert an interface number (see the Note on **page 2-22**) into every timeslot being used (in the example shown in **Figure 2-11**, 16 timeslots are used, the rest have zeros in them). Type the number, press ENTER, then use the arrow keys to highlight the next timeslot field. Exit this field by using the arrow keys.The cursor automatically moves to the **T1 Line Coding** field.



The value assigned to the timeslots is the interface being used for WAN communication. The next available interface is displayed on the WAN Physical Configuration screen in the Next IF field (see **Figure 2-3**). The Next IF number shown must be used to add a new interface. The Next IF will increment as interfaces are added. The previously entered interfaces can be modified by entering the interface number.

The following four steps are based on information supplied by the service provider. Consult the service provider for the correct settings.

5. Use the arrow keys to highlight **T1 Line Coding**. Use the SPACE bar to select **B8ZS** or **AMI**, then press ENTER.
6. Use the arrow keys to highlight **T1 Frame Type**. Use the SPACE bar to select **ESF** or **D4**, then press ENTER.

7. Use the arrow keys to highlight **T1 Tx Clock Source**. Use the SPACE bar to select **Local** (no clock source provided by telephone company) or **Loop** (clock source provided by telephone company), then press ENTER.

If you are using a Local clock source, set only one end of the circuit for Local, the other end must be set for Loop.

8. Use the arrow keys to highlight **T1 Line Buildout** (LBO). Press the SPACE bar to select **0 dB** unless the service provider recommends another setting, then press ENTER.
9. Use the arrow keys to highlight **T1 Network Loopback**. Press the SPACE bar to select **None**, then press ENTER.
10. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory. The host platform reboots, and re-entry to Local Management is necessary for any further configuration.
11. Proceed to the next section to continue configuration.

T1 Interface Configuration

The WAN Interface Configuration screen is accessed through the WAN Physical Configuration screen. Access the WAN Interface Configuration screen by using the arrow keys to highlight the **WAN INT CONFIG** command and press ENTER. Refer to **Figure 2-6** and proceed with the following steps to configure the WAN Interface.

1. Set the WAN connection Interface Number by typing the same number into the **Interface Number** field that was input into the timeslots in the WAN Physical Configuration screen, then press ENTER (see the Note on **page 2-22**).
2. Unless the user sets the Max Xmit Unit, the HSIM or CyberSWITCH automatically sets the **Max Xmit Unit** to **1526** (default) after the active protocol (PPP) is selected.
3. Make any changes to the available settings as desired.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory.

The WAN configuration is complete. It takes up to 60 seconds for the WAN Interface to come out of standby and for communications to begin.

Configuration: Frame Relay

This section provides step-by-step instructions for configuring the HSIM or CyberSWITCH to use a T1 circuit in a Frame Relay environment. This example assumes the setup shown in **Figure 2-12** using two CSX400s, each with an HSIM or CyberSWITCH installed. Configurations may vary depending on the host platform.

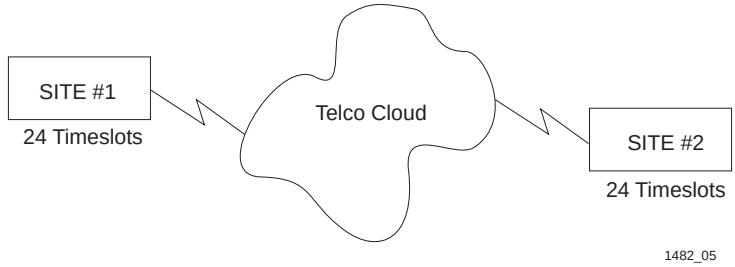


Figure 2-12 Frame Relay Configuration

The line configuration information shown in **Table 2-3** must be supplied by the service provider.

Table 2-3 Telco Configuration Information

Configuration Information Required by Customer	Information Supplied by Service Provider
Line Coding	B8ZS or AMI
Frame Type	ESF or D4
Clock Source	Loop Timing or Local Timing
DS-0s (Timeslots)	Timeslots being used for each end of the circuit

Frame Relay Physical Configuration

Begin the HSIM or CyberSWITCH physical configuration by accessing the **WAN Physical Configuration** screen through Local Management (**Figure 2-6**). Proceed with the following steps:

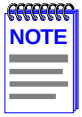
1. Use the arrow keys to highlight the **[WPIM X]** field at the bottom of the screen. Press the SPACE bar to select the number of the WPIM to be configured, then press ENTER.
2. Use the arrow keys to highlight the **MgrType** field. Configure the Protocol Manager Type as either Frame Relay Point to Multipoint (FR PtoMP), or Point to Point (FR PtoP).

FR PtoMP and FR PtoP are the two settings for Frame Relay. Frame Relay Point to Point has one Interface per DLCI assigned when DLCIs are created by the Service Provider. In Frame Relay Point to Multipoint, there is one interface to multiple DLCIs, and the DLCIs are dynamically learned. When backing Up a Frame Relay Primary circuit it is best to configure the Frame Relay protocol manager for Point to Point mode. If the Primary Frame Relay interface has only one DLCI it can work in Point to Multi-Point mode.

The concept of a Manager for each configured protocol also exists. Each physical connection has one or more (more if a protocol is encapsulated, such as PPP encapsulated within ISDN) Protocol Managers that control protocol operation.

Point to MultiPoint Configuration (LM WAN Physical Configuration)

1. Set the MgrType to FR PtoMP.
2. If more than 32 DLCIs are required, set the Max VCs value (up to a maximum of 125 on the CSX400/HSIM-W6).

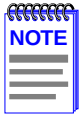


The MAX VC value associated with a physical WAN interface is set to a default value based on the number of possible ports available and the protocol manager selected. If more PVCs/DLCIs exist than the default MAX VC value will allow, the MAX VCs may be changed.

3. The next IF will display the value that should be entered into the timeslots, if T1 or E1. This should be done now.
4. Configure any other required physical parameters for that interface. Such as: Sync Port Type, or clock speeds (Sync WPIM), T1 or E1 timeslot configurations etc. REMEMBER: if using the Sync WPIM, always manually setup the Sync Clock Speeds to match the actual line configurations.

Point to MultiPoint Configuration (LM WAN Interface Configuration) LMI Type

1. If the LMI type required is ANSI T1-617 Annex D version 1994, no more configuration is needed. It is recommended that the box be reset after the DLCIs are known by the HSIM or CyberSWITCH. The DLCIs will show up on the LM Interface screen when they are sent in STATUS messages from the FR switch.
2. If another selection is required this can be done by toggling the FR LMI (Link Mgt Protocol) field.



If you toggle the LMI type, all DLCI information will be removed.

Point to MultiPoint Configuration (DLCI Address)

1. If the DLCI LMI type is NO_LMI, or you wish to have STATIC DLCIs (that will not have information deleted when the switch does not send a report on them, or if QUICKSET configured the DLCIs), then you would add the DLCIs using this field.
2. Type in the DLCI number you wish to use here, and arrow down to the Circuit State. Add the DLCI in the inactive state (if NO_LMI it can be added in the active state) and SAVE. The DLCI will show up as a STATIC DLCI.
3. If a switch is attached the DLCI should dynamically change state to active, and then data can be received and transmitted. In NO_LMI mode, the state must be changed manually.
4. To remove a STATIC DLCI, arrow to the Circuit State field and select invalid and SAVE. This will remove the DLCI from the system. NOTE: This does not apply to DYNAMIC DLCIs.(c) CKT_DCP enable: This will turn Fr Data Compression negotiation on or off. The next two fields, Status and ratio, display whether or not DCP successfully negotiated. If successful, the Compression ratio is displayed.

In Point To MultiPoint mode the DLCIs will be dynamically added (unless the DLCI has been tagged STATIC or deleted. This allows you to actually see the DLCI information provided by the Frame Relay DCE Switch in the WAN cloud that the CSX is connected to.

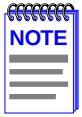
Point To Point Mode (LM WAN Physical Configuration)

Set the MgrType to FR PtoP. All the other information in FR PtoMP configuration is applicable.

Point To Point Mode (LM WAN Interface Configuration)

The difference in configuration between PtoP and PtoMP is that DLCIs are not learned dynamically. DLCI information must be entered in statically, even if in an LMI mode. All the other information in FR PtoMP configuration is applicable.

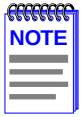
Since in Point To Point mode the DLCI is static, it will not be deleted if the switch sends no information on the DLCI, but must be deleted manually through LM or SNMP, nor will DLCIs be added dynamically. The state will reflect the correct value that the FR DCE Switch reports, and static circuits will go “Invalid” if there is a physical connection problem.



When changing from one protocol to another on a HSIM or CyberSWITCH that has been operational, save NONE as the protocol before changing to another protocol.

The previous version of firmware allowed multiple Frame Relay Protocols running on different T1 or E1 channel groups. This is no longer possible. Therefore, only one Frame Relay Protocol can be configured per physical interface.

5. Use the arrow keys to highlight **Timeslot View**. Press the SPACE bar to select **New**, then press ENTER. The cursor moves to the first timeslot available in the Timeslot Configuration Table.
6. Insert the interface number (refer to NOTE below) into the timeslot being used. Type the number, press ENTER, then exit this field by using the arrow keys. The cursor automatically moves to the **T1 Line Coding** field.



The value assigned to the timeslots is the interface being used for WAN communication. Only one interface can be assigned to the timeslot when running Frame Relay.

The next four steps are based on information supplied by the service provider. Consult the service provider for the correct settings.

7. Use the arrow keys to highlight **T1 Line Coding**. Press the SPACE bar to select **B8ZS** or **AMI**, then press ENTER.
8. Use the arrow keys to highlight **T1 Frame Type**. Press the SPACE bar to select **ESF** or **D4**, then press ENTER.
9. Use the arrow keys to highlight **T1 Tx Clock Source**. Press the SPACE bar to select **Local** (no clock source provided by telephone company) or **Loop** (clock source provided by telephone company), then press ENTER.

10. Use the arrow keys to highlight **T1 Line Buildout** (LBO). Press the SPACE bar to select to **0 dB** unless the service provider recommends another setting, then press ENTER.

11. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message “SAVE DONE!” displays and Local Management saves the changes to memory. “REBOOT IN PROGRESS.....” displays and the host platform reboots. Re-entry to management is necessary for any further configuration.

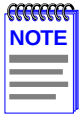
12. Proceed to the next section to continue the configuration.

Frame Relay Interface Configuration

Access the WAN Interface Configuration screen through the WAN Physical Configuration screen, by using the arrow keys to highlight the **WAN INT CONFIG** command, then press ENTER. Proceed with the following steps to configure the WAN Interface.

1. Set the Interface Number that is being used for the WAN connection by typing the same number into the **Interface Number** field that was input into the timeslots in the WAN Physical Configuration screen, then press ENTER (see the Note on page 2-27). For Frame Relay PtoP: The interfaces are assigned when DLCIs are created (in this case a zero needs to be entered in this field).

2. Use the arrow keys to highlight **FR LMI**. Press the SPACE bar to select **ANSI_94**, **T1.617-D** or **Q.933-A**, then press ENTER.



The choice NO LMI under FR LMI is a test mode only and should not be used in a practical application.

3. Make any changes to the available settings as desired.

4. Use the arrow keys to highlight **SAVE**, then press ENTER. The message “SAVE DONE!” displays and Local Management saves the changes to memory.

In FR PtoP, the DLCIs must be entered statically, as they will not come up dynamically as in FR PtoMP.

In FR PtoMP, there is an option to statically enter the DLCIs in association with a Protocol Manager, the physical port and MIB II, using the DLCI field in the Interface screen. If the DLCI is not static, it will be deleted if the Frame Relay switch determines that the DLCI has been eliminated. If the Frame Relay switch previously reported status on a DLCI, when it does not report the status of the DLCI, the DLCI and its associated information is deleted from the platform. Static entries are never deleted automatically. They must be deliberately deleted by the user. To enter a DLCI, it is set to “Inactive” and saved, but to delete a DLCI, it must be accessed and entered as “Invalid” and saved.

The WAN configuration for Frame Relay is complete. Communications between the HSIM or CyberSWITCH and the service provider’s switch takes approximately one or two minutes to complete. A status of **Inactive** displays on a DLCI per DLCI basis by default until both ends of the DLCI are configured correctly. Once both end devices have negotiated link management with the switches, and are configured correctly on a DLCI per DLCI basis, the status field displays **Active**.

Configuration: DDS Service

This section provides step-by-step instructions for connecting the HSIM or CyberSWITCH to a Digital Data Service circuit in a PPP or Frame Relay environment. This example assumes the setup similar to the one shown in **Figure 2-13** using two CSX400s with HSIM or CyberSWITCH modules installed.

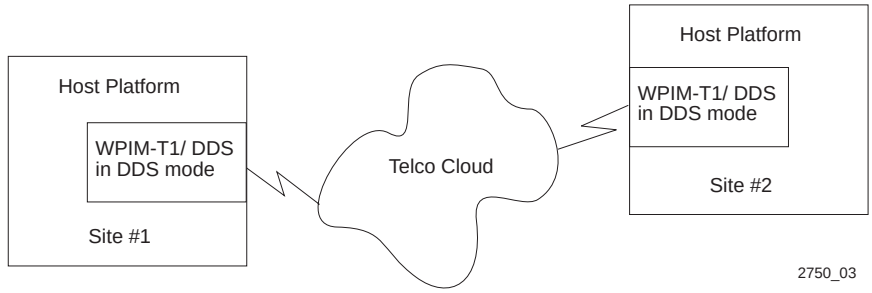


Figure 2-13 WPIM-DDS Interface Configuration for PPP

The line configuration information shown in Table 2-4 must be supplied by the service provider.

Table 2-4 Telco Configuration Information

Configuration Information Required By User	Configuration Information Supplied By Service Provider
Clock Source	Telco provided or no clock source
Line Mode	Primary or Clear Channel
FR-LMP (Frame Relay Only)	Telco provided or user requested

DDS Service Physical Configuration

Begin the DDS configuration by accessing the WAN Physical Configuration screen (Figure 2-14) through Local Management. To access the WAN Physical Configuration screen, use the arrow keys to highlight the **WAN Setup** option, then press ENTER. The screen shown in Figure 2-14 displays.

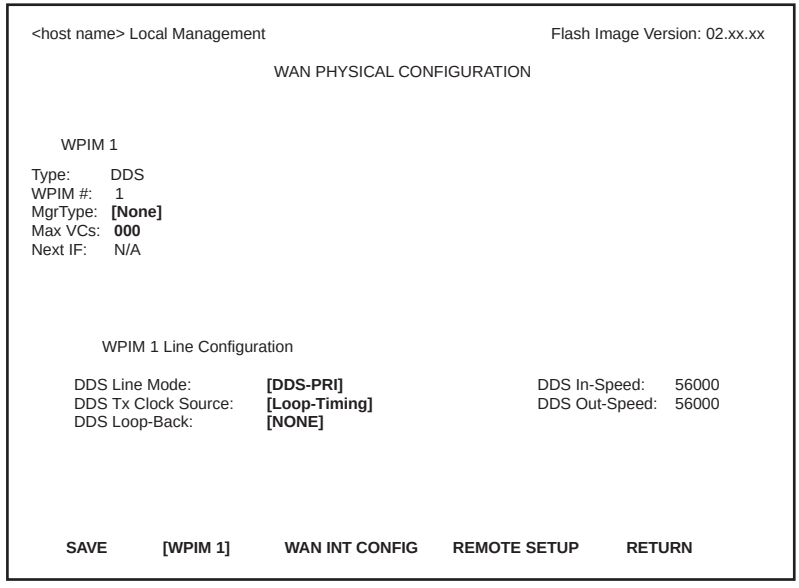


Figure 2-14 WAN Physical Configuration Screen for DDS Service

Proceed with the following steps:

1. Use the arrow keys to highlight the **WPIM X** field at the bottom of the screen. Press the SPACE bar to select the number of the WPIM being configured, then press ENTER.
2. Use the arrow keys to highlight **MgrType**, and choose the Protocol Manager from **PPP**, **FR PtoMP**, **FR PtoP**, or **HDLC** using the space bar to toggle the selections.

When changing from one protocol to another on a WPIM-T1/DDS that has been operational, save NONE as the protocol before changing to another protocol.

3. Use the arrow keys to highlight **DDS Line Mode**. Press the SPACE bar to set the DDS Line Mode to **DDS-PRI** or **DDS-CC**, then press ENTER.
4. Use the arrow keys to highlight **DDS Tx Clock Source**. Press the SPACE bar to set to **Loop-Timing**, then press ENTER.
5. Use the arrow keys to highlight **DDS Loop-back**. Press the SPACE bar to set to **NONE**, then press ENTER.
6. Use the arrow keys to highlight the **SAVE** command. Then press ENTER. The message “SAVE DONE!” displays and Local Management saves the changes to memory. “REBOOT IN PROGRESS.....” displays and the host platform reboots. Re-entry to management is necessary for any further configuration.

DDS Service Interface Configuration

The WAN Interface Configuration screen is accessed through the WAN Physical Configuration screen. Access the WAN Interface Configuration screen (**Figure 2-6**) by using the arrow keys to highlight the **WAN INT CONFIG** command, then press ENTER. Proceed with the following steps to configure the WAN Interface through Local Management.

1. Use the arrow keys to highlight **Interface Number**. Set the WAN connection Interface Number by typing the same number found in the Interface field on the WAN Physical Configuration screen into the Interface Number field, then press ENTER.
2. If Frame Relay was selected, use the arrow keys to highlight **FR LMI**. Press the SPACE bar to select **ANSI_94**, **NO LMI**, **T1.617-D**, or **Q.933-A**, then press ENTER.

If NO LMI was selected, complete the following:

- Use the arrow keys to highlight **DLCI Address**. This field can be set to values from 0-1023. The values 16-991 are typically used for virtual circuits.
- Use the arrow keys to highlight **Circuit State**. Press the SPACE bar to select Active, then press ENTER.

3. If PPP was selected as the Protocol Manager instead of Frame Relay, the Max Xmit Unit setting may be changed from the default of 1526 if desired.
4. Make any changes to the available settings as desired.
5. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory.

The WAN configuration is complete for DDS service. Communication between the HSIM or CyberSWITCH and the service provider’s switch takes approximately one to two minutes to complete. A status of **Inactive** displays on a DLCI per DLCI basis by default until both ends of the DLCI are configured correctly. Once both end devices have negotiated link management with the switches, and are configured correctly on a DLCI per DLCI basis, the status field displays **Active**.

Troubleshooting the Frame Relay Connection

There are three troubleshooting tools on the HSIM or CyberSWITCH platform.

- LM
- The FR Error MIB Table, and reflects LMI or DLCI data errors
- The Mib Navigator command “fr”

A discussion of what is provided by the FR DTE bridge/router and the FR DCE switch needs to be clarified:

Communication with the FR switch is done through one of two methods:

- Asynchronous Status Messages. At any time the Fr Switch can send an unsolicited (no polling from us) message to us. Each message contains information on one DLCI and one only. It has the DLCI number and the DLCI state. We don't respond to this message, but we do adjust what we know about DLCIs based on this information.

- Synchronous Polling Messages. The t391 timer for ANSI/ITU Frame Relay forms the basis for polling between the FR switch and the FR DTE (us). We transmit a STATUS ENQUIRY every t391 seconds (10 by default) to the FR switch. We expect a STATUS RESPONSE before we reach our next t391 polling cycle. The very first time we transmit a STATUS MESSAGE, and every successive N391 times (6 by default) we send out a FULL STATUS ENQUIRY. We expect a FULL STATUS RESPONSE, which contains information on the DLCIs the switch has assigned to us. Every other T391 cycle we send out a LINK INTEGRITY VERIFICATION ENQUIRY message (LIV). We expect to get a LINK INTEGRITY VERIFICATION RESPONSE back from the Fr switch before out t391 polling cycle expires. This is a keep alive message that does no more than let us know the link between us and the FR switch is still alive.

The information provided in a FULL STATUS RESPONSE, or ASYNCHRONOUS STATUS MESSAGE basically has two parts, the FR Switch provides a DLCI number, and whether that DLCI is in the Active or Inactive state.

- The Active state means that both ends of the connection (this DTE and the DTE at the other end of the WAN cloud) are speaking correctly to the FR DCE Switches in the WAN cloud.
- The Inactive state means that either the local or far end DTE is either just starting up and has not completed its initial negotiation with the FR Switch, or there is some sort of LMI error. Data (other than LMI negotiation messages) will only be transferred when in the Active state.
- A third state value, Invalid, is reported locally only. It is not done by polling the FR switch. This is done if the physical connection has some sort of problem. The circuit will remain in the Invalid state until negotiation with the FR DCE Switch completes successfully.

FR Error Table

This table is a standard part of RFC 2115, and provides the following information on a physical interface per physical interface basis:

- The time of the failure: (value of Mib II sysUpTime)
- The type of failure

receiveShort:	The frame was not long enough to allow demultiplexing - the address field was incomplete, or for virtual circuits using Multiprotocol over Frame Relay, the protocol identifier was missing or incomplete.
receiveLong:	The frame exceeded maximum length configured for this interface.
illegalAddress:	address field did not match configured format.

unknownAddress:	frame received on a virtual circuit which was not active or administratively disabled.
dlcmiProtoErr:	unspecified error occurred when attempting to interpret link maintenance frame.
dlcmiUnknownlE:	link maintenance frame contained an Information Element type which is not valid for the configured link maintenance protocol.
dlcmiSequenceErr:	link maintenance frame contained a sequence number other than the expected value.
dlcmiUnknownRpt:	link maintenance frame contained a Report Type Information Element whose value was not valid for the configured link maintenance protocol.
noErroSinceReset:	no errors have been detected since the last cold start or warm start.

- The number of times the interface has gone down due to faults
- The value of sysUpTime when the interface last went down due to errors.

Configuration: Call Backup

This section provides instructions for configuring the HSIM or CyberSWITCH to automatically backup a PPP dedicated/permanent connection or a Frame Relay PVC using a dial-up ISDN. These are the two primary uses. All connections configured as call backup are continuously monitored for a failed condition. Whenever a primary connection with call backup fails, the backup call is automatically made using Dial-on-Demand (DoD). Once the failed connection is restored the backup call may be automatically closed. DoD automatically brings up the backup SVC connection whenever the primary connection has failed and there is traffic to be forwarded across the backup SVC.

This example assumes the setup shown in **Figure 2-15**, using two CSX400s with primary connections using WPIM-T1s (WPIM-E1, WPIM-DDS, or WPIM-SY could also be used) and with HSIM or CyberSWITCH backup modules installed in each CSX400. The NT-1 is needed if the connection to the Telco cloud has a U interface.

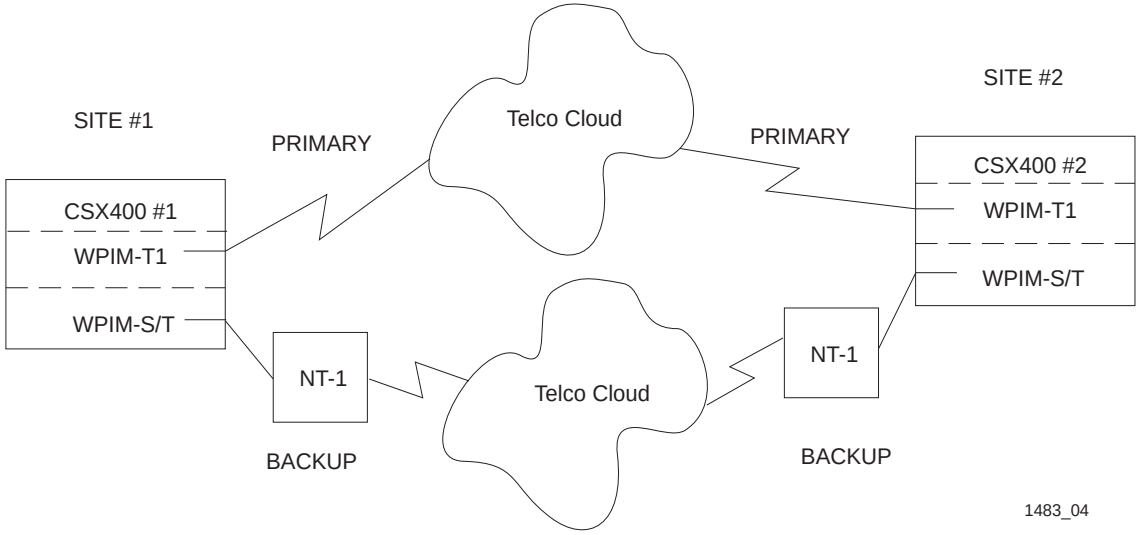


Figure 2-15 Configuration for PPP backup

The procedures listed below and detailed in the following sections must be performed in the order given to properly configure the HSIM or CyberSWITCH for call backup:

- Configure primary lines and routing.
- Select the protocol.
- Enable CCP.
- Configure backup.
- Set idle timeouts.
- Configure the D channel.
- Set phone numbers and SPIDS (if applicable).
- Set maximum number of neighbor/remote profiles.
- Configure the profiles.
- Reset the device.
- Verify status.

NOTE

Network Tools can be found in the MIB NAVIGATOR selection in the main menu of Local Management for the host platform.

Configure Primary Lines and Routing

Configure the primary lines. Refer to the appropriate WPIM user's manual. Configure routing if used. Refer to the appropriate host platform user's manual.

Select the Protocol

Select the ISDN Protocol Manager for the HSIM or CyberSWITCH in Local Management, using the WAN Physical screen.

Begin the HSIM or CyberSWITCH configuration by accessing the WAN Physical Configuration screen through Local Management. Access the WAN Physical Configuration screen from the WAN Setup menu item that displays in the Setup Menu in Local Management. Use the arrow keys to highlight the **WAN Setup** menu item, then press ENTER. The screen shown in **Figure 2-16** displays.

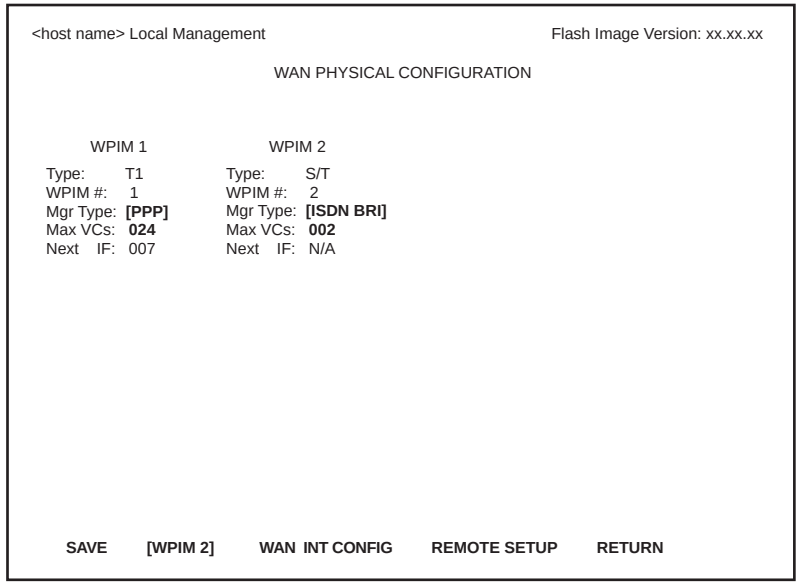
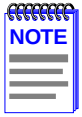


Figure 2-16 WAN Physical Configuration Screen

Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM X]** field at the bottom of the screen. Press the SPACE bar to select the WPIM number of the HSIM or CyberSWITCH being configured, then press ENTER. Typically the backup HSIM or CyberSWITCH will be installed in slot 2 of the host platform.
2. Use the arrow keys to highlight the **MgrType**. Press the SPACE bar to select ISDN BRI, then press ENTER.



The MAX VC value associated with a physical WAN interface is set to a default value based on the number of possible ports available and the protocol manager selected. If more PVCs/DLCIs exist than the default MAX VC value will allow, the MAX VCs may be changed.

3. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message “Save Done” displays and Local Management saves the changes to memory. The message “REBOOT IN PROGRESS.....” will also display, and the host platform will automatically reboot.

Enable Compression Control Protocol (CCP)

The WAN Interface Configuration screen, **Figure 2-17**, need only be accessed if the Compression Control Protocol (CCP) feature is to be turned on (normally it is desirable to have this function on). Otherwise, the functions of this screen are not normally needed for call backup. Access the WAN Interface Configuration screen by using the arrow keys to highlight the WAN Int Config command in the WAN Physical Configuration screen, then press ENTER.

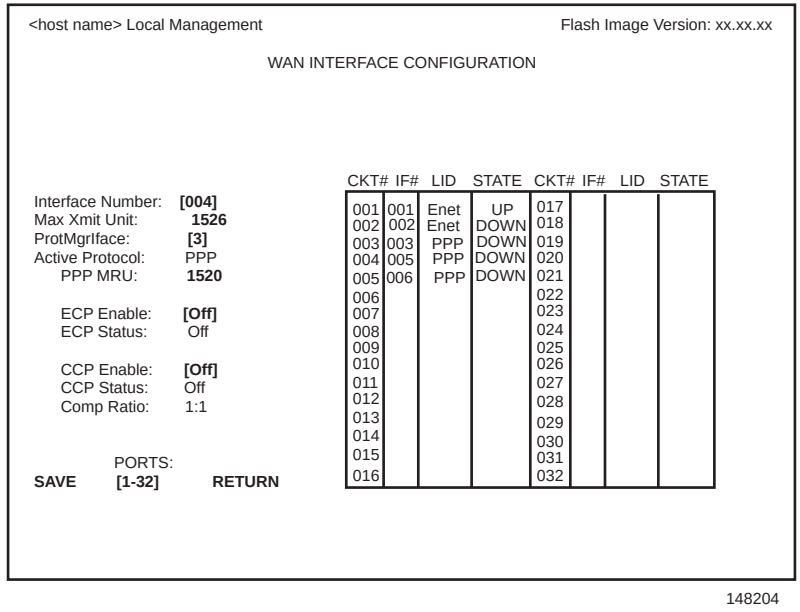


Figure 2-17 WAN Interface Configuration Screen

Proceed with the following steps:

1. Use the arrow keys to highlight **Interface Number**. Set the WAN connection Interface Number by typing the number of the interface to configure (from the IF# column), then press ENTER.
2. Use the arrow keys to highlight **CCP Enable**. Press the SPACE bar to select **On** to enable CCP, then press ENTER.
3. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory. Upon saving this screen, the configured interface is assigned to an application port (CKT#) displayed in the table. The connection will display active status (UP) once the device starts communicating with the service provider’s switch.

The commands in the rest of the procedure are Network Tools commands. Refer to the host platform manual for detailed information on accessing Network Tools.

Configure Backup

Backup is normally used to configure a backup connection if a primary connection fails. It can also be used to reduce CPU time for an unused interface. Use the following Network Tools command to configure backup:

setbackup [PRIMARYIFACENUM] [BACKUPIFACENUM] [TIMETOCONNECT] [TIMETODISCONNECT] [CONNECTRETRIESNUM] [TIMEBETWEENCONNECTRETRIES] [BACKUPOVERRIDE]

PRIMARYIFACENUM — The number of the primary interface that is going to be backed up.

BACKUPIFACENUM — The number of the interface assigned as the backup interface to the primary interface.

TIMETOCONNECT — How long the system will wait (in seconds) before attempting to switch over to the backup interface. Default is zero. Allowed values are in increments of five seconds.

TIMETODISCONNECT — How long the system will wait (in seconds) before attempting to switch over to the primary interface once the primary interface has been restored. Default is 90 seconds. Allowed values are in increments of five seconds.

CONNECTRETRIESNUM — Specifies the number of tries to bring up the backup interface before giving up. The default is three. Allowed values are in increments of one.

TIMEBETWEENCONNECTRETRIES — Specifies the time interval between tries to bring up the backup interface. The default is 30 seconds. Allowed values are in increments of five seconds. Values below 30 seconds are allowed but not advisable.

BACKUPOVERRIDE — Specifies if the backup interface will disconnect whenever the primary interface is restored (reconnected). Choosing ENABLED for this command will not disconnect the backup interface even though the primary interface is restored. Used specifically when the primary interface has an intermittent problem, as it is desirable for the backup interface to stay connected until the primary interface problem is corrected. Once the primary connection is fully operational, BACKUPOVERRIDE should be set to DISABLED, the default value.

Example 1:
There is a nailed-up PPP interface #3, and to back it up, ISDN interface #4 is used with the default values. Use the command:

setbackup 3 4

Example 2:

For any switched medium like ISDN there are two types of interfaces, primary and secondary (backup). Primary interfaces automatically attempt to connect using DoD. Because of this, it is recommended not to create any unnecessary interfaces because they will consume unnecessary time in trying to connect. However, if additional interfaces have been created for which their need is unknown, then DoD should be disabled. To do this, set the backup interface to itself. Do this for each interface that should have DoD disabled. This recommendation also applies to Dial-in only interfaces (i.e., answer mode interfaces). Use the command:

setbackup 3 to 3

Answer mode only is set, a “dormant” state. This will set the backup interface to itself if the ISDN interface is to be used only as a dial-in circuit (i.e., answer mode only).

If the interface is active, you cannot configure backup. De-activate the interface before proceeding.

Set Idle Timeouts

Set the receive and transmit idle timeouts for backup interfaces using Network Tools. This command automatically disconnects an idle switched interface when either one of the parameters TRANSMITIDLETIMEOUT or RECEIVEIDLETIMEOUT is met for the interface:

setidletimeout [IFACENUM] [TRANSMITIDLETIMEOUT] [RECEIVEIDLETIMEOUT]

IFACENUM — The number of the interface to be configured.

TRANSMITIDLETIMEOUT — The idle time out parameter for the transmit time out.

RECEIVEIDLETIMEOUT — The idle time out parameter for the receive time out.

Example: To set the receive time out to 180 seconds and the transmit side to 600 seconds for ISDN interface #4, use this command:

setidletimeout 4 180 600

Configure the D Channel

Use the following command in Network Tools to set the switch type:

setswitchtype [WANPORTNUM] [SWITCHTYPE]

WANPORTNUM — If the HSIM or CyberSWITCH occupies WAN port number one, use 1, if it occupies port number two, use 2 as the WANPORTNUM.

SWITCHTYPE — Choose between the types of ISDN BRI switches. The choices are NI1 (default for BRI), DMS100 (BRI/PRI), ATT5 ESS (BRI/PRI, default for PRI), ATT-4ESS (PRI) and NET3 (BRI).

Set Phone Numbers and SPIDs for the Port

The following Network Tools command is used to set the phone numbers and the SPIDs (if applicable):

setisdnbri [WANPORTNUM] [LDN1][SPID1] [LDN2] [SPID2]

LDN1 — The first Local Directory Number. Likewise, LDN2 is the second Local Directory Number.

SPID1 — The first Service Profile Identifier. Likewise, SPID2 is the second Service Profile Identifier.

SPID format: [XXXYYYZZZZ] [01] [01]

Where XXX represents the area code, YYY represents the prefix, and ZZZZ represents the local number. [01] [01] is the fixed suffix. This is the proposed generic SPID format.

Example 1: For the first WAN port to be configured for ISDN, issue the command:

setisdnbri 1 5551000 0555100001 5553000 0555300001

For the second WAN port to be configured, issue the command:

setisdnbri 2 5551000 0555100001 5553000 0555300001

The command also allows for skipping or clearing any entry by using the key letters S (or s) to skip the field, and C (or c) to clear the field.

Example 2: To skip LDN1 and SPID1, change LDN2, and clear SPID 2, issue the following command:

setisdnbri 2 s s 0555600001 c

Set Maximum Number of Neighbor/Remote Profiles

A neighbor/remote profile describes a possible connection. The maximum should be set to account for support of PPP Multilink. If PPP Multilink is used, then the number of profiles must accommodate the maximum possible number of additional “more BW” connections/calls desired. Consequently, each neighbor profile would then describe a possible connection to the same remote end point (user). In the example, two profiles will be set up for the first ISDN interface. This means that this ISDN interface can be used to connect (call) two different end users or the same end user twice (e.g., Multilink). The default is one profile per ISDN interface.

Use the Network Tools command:

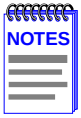
setmaxprofiles [IFACENUM] [MAXPROFILESNUM]

Example: To set two profiles for ISDN interface #4 issue the command:

setmaxprofiles 4 2

Configure the Profiles

Configure the profiles and specify phone numbers for backup interfaces. Use Local Management to configure BoD (submenu of the profiles menu) and enable using MLP if desired. Refer to **Remote Profiles Setup** for details.



Set max profiles, total profiles to allow multilink (QuickSET does this automatically).

Multilink is dynamic and will automatically create an interface to support the link.

Verify Status

Use the Network Tools command idsnstat to verify the D channel status; it should read active. The isdnstat command is used to display the ISDN settings, including the switch type, LDNs, SPIDs, and the operational status of the D channel. This command is normally used to verify that the switch and the HSIM or CyberSWITCH are working properly. If the settings are not correct, or the D channel is not operational, the situation must be corrected before continuing the configuration. The connection must be operational or the backup configuration will not work.

isdnstat [WANPORTNUM]

Use the Network Tools commands ct and dt to test the line by doing a manual connect or disconnect:

ct [IFACENUM] connects (places) a call for the interface designated.
dt [IFACENUM] disconnects (hangs up) the call.

These three Network Tools commands allow the user to check whether or not the ISDN line and profile(s) have been configured properly and that a connection is possible.

When reconfiguring an interface, the host platform does not have to be reset.

Configuration is complete.

Reset

If the Telco must be re-initialized, the host platform must be reset or the ISDN line must be disconnected. Refer to the host platform user's guide to reset the platform.

3 MIB Navigator

This chapter explains how to use the MIB Navigator utility. The MIB Navigator allows access to a command set from which you can configure and manage your HSIM or CyberSWITCH.

Chapter Organization

The following list summarizes the organization of this chapter:

MIB Navigator Screen – describes the MIB Navigator screen and explains how to access it.

MIB Navigator Command Set Overview – describes the types of commands available to the MIB Navigator.

Navigation Commands – explains the commands used to navigate through the MIB Navigator.

PPP Security Command – explains how to list and set security on an interface basis.

Spoofing Command – explains how to set spoofing for an interface.

ISDN Configuration Commands – explains how to set up primary and backup configurations.

Other Commands – explains other commands that allow you to access and manage network devices connected to the device running the MIB Navigator.

Special Commands – explains the special commands that allow you to exit from the MIB Navigator.

MIB Navigator Screen

Access the MIB Navigator screen from the Main Menu screen using Local Management (refer to the **Accessing Local Management** section in **Chapter 1**). Using the arrow keys, highlight the **MIB NAVIGATOR** menu item, then press ENTER. At the MIB Navigator cursor, type **Help** and press ENTER. The MIB Navigator Help screen shown in **Figure 3-1** displays.

```
Welcome to MIB Navigator

MIBNav-> help

Commands Available to the User :

Navigation commands :
 branch    cd        ctron     dir       get       grep
 ls        mib2      next      pwd       set       su
 tree      wan       whoami

PPP Security Configuration:
 pppsecurity

Spoofing activation/setup command:
 setspoof

Isdn configuration, primary/backup setup commands :
 setbackup       setisdnbri        setswitchtype    ct
 dt              setidletimeout    setalarmtime     setmaxprofiles
 setdemandif     isdnstat          ic

Other commands :
 arp             bridge       circuitmap   defroute    dhcp         ds1alarm
 fr              imux         nat          netstat     ping         ppp
 redistribute    reset        route        secondIP    show         snmpbranch
 snmpget         snmpnext     snmpset      snmptree    traceroute   wanpq

SPECIAL :
 done, quit, or exit - Exit from the MIB Navigator.
 mib2  - Change directory to MIB II (/1/3/6/1/2/1).
 ctron - Change directory to Cabletrons MIB (/1/3/6/1/4/1/52)

 wan - Change directory to Cabletrons WAN MIB (/1/3/6/1/4/1/52/4/1/2/7/2)
For help with a specific command, type 'help <command>'.

MIBNav->
```

Figure 3-1 MIB Navigator Help Screen

Managing Device MIBs

The MIB Navigator lets you manage objects in the HSIM or CyberSWITCH Management Information Bases (MIBs). MIBs are databases of objects used for managing the device and determining the device's configuration. The commands within the MIB Navigator enable you to view and modify a device's objects.

The MIB Navigator views the MIB tree hierarchy as a directory. Figure 3-2 shows the MIB tree hierarchy. Each layer is numerically encoded, so that every branch group and leaf object in the MIB is identified by a corresponding number, known as an Object Identifier (OID). This allows the MIB Navigator to navigate through the MIB and access the manageable leaf objects.

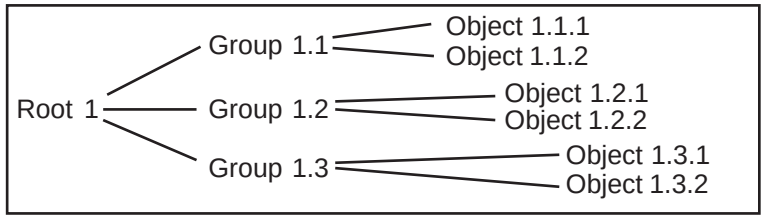


Figure 3-2 Hierarchical MIB Tree Structure

Often an ASCII name is assigned to the OID of a leaf object, making it more readable. To identify the value for the object “ipForwarding” you use the OID (/1/3/6/1/2/1/4/1), or its ASCII name (/iso/org/dod/internet/mgmt/mib-2/ip/ipForwarding).

MIB Navigator Command Set Overview

TIP

Use the help command for an on-line description of each MIB Navigator command. For example **MIB Nav-> help branch** provides help information for the branch command. The help command can also be used alone to display the available commands, as seen in Figure 3-1. A command used incorrectly (wrong syntax) will prompt a display of the correct usage. Use lower case characters when entering commands in Network Tools.

The MIB Navigator command set provides the following commands:

Navigation Commands — Navigation commands allow you to access and manage the MIB for the device running the MIB Navigator. Some of these commands also provide user community-string information. The commands, detailed starting on page 3-3, are as follows:

branch	cd	ctron
dir	get	grep
ls	mib2	next
pwd	set	su
tree	wan	whoami
help		

PPP Security and Spoofing Commands — Commands that allow you to set PPP security and to set up spoofing. The commands, detailed starting on **page 3-14**, are as follows:

pppsecurity	setspoof

ISDN and Backup Commands — Commands that allow you to configure ISDN, and setup primary and backup configurations. The commands, detailed starting on **page 3-16**, are as follows:

setbackup	setisdnbri	setswitchtype	ct
dt	setidletimeout	setalarmtime	setmaxprofiles
setdemandif	isdnstat	ic	

Other Commands — Other commands allow you to access and manage network devices connected to the device running the MIB Navigator. The commands, detailed starting on **page 3-20**, are as follows:

arp	bridge	circuitmap	defroute
dhcp	ds1alarm	fr	imux
nat	netstat	ping	ppp
redistribute	reset	route	secondIP
show	snmpbranch	snmpget	snmpnext
snmpset	snmptree	traceroute	wanpq

Special Commands — Special Commands allow you to exit from the MIB Navigator. The commands, detailed starting on **page 3-35**, are as follows:

done	quit	exit

Conventions for MIB Navigator Commands

This manual uses the following conventions for denoting commands:

- Information keyed by the user is shown in this helvetica font.
- In the examples, information keyed in by the user is indicated by **bold font**.
- Command arguments are indicated by two types of brackets:
  - required arguments are enclosed by [ ].
  - optional arguments are enclosed by < >.

MIB Navigator command conventions are as follows:

- To abort the output or interrupt a process the escape character is ^C (where ^ indicates the Control key).
- A slash (/) preceding an OID issues that command from the root directory regardless of where you are in the MIB. If no slash precedes the OID the command issues from your current MIB location.
- Dot notation (1.1.1.1) is equivalent to slash notation (1/1/1/1). Use slash notation with the navigational commands, and the dot notation with the built-in commands that are using SNMP to access and manage network devices.

MIB Navigation Commands are listed in the format shown below:

command:

Syntax:	This entry provides the format that the MIB Navigator command requires. It indicates where arguments, if any, must be specified.
Description:	This entry briefly describes the command and its uses.
Options:	This entry lists any additional fields which may be added to the command and their format.
Example:	This entry shows an example of the command.

Navigation Commands

The following MIB Navigation commands allow you to move from MIB object to MIB object within the MIB tree.

branch:

Syntax: branch [path]

Description: The branch command displays all of the leaves in the MIB tree below a specified path. The information displayed includes the pathname, the object ASCII name, the type of object (i.e., integer, counter, time tick, etc.), and the current value of each leaf object.

Options: Not Applicable

Example:

```
MIBNav-> branch

# /1/3/6/1/2/1/7/1    udplnDatagrams    COUNTER   28216
# /1/3/6/1/2/1/7/2    udpNo Ports        COUNTER   0
# /1/3/6/1/2/1/7/3    udplnErrors        COUNTER   0
```

cd:

Syntax: cd [path] or cd <option>

Description: The cd command allows you to change directories within a MIB subtree (branch). The path specified must be valid, or the MIB Navigator will not perform the cd operation.

Options: .. Moves you one subtree above the current one.

/ Moves you to the root.

Example:

```
MIBNav-> cd missing/iso/org/dod/internet/mgmt
```

ctron:

Syntax: ctron

Description: The ctron command allows you to change directories to the Cabletron MIB (1.3.6.1.4.1.52) without keying in the entire path.

Options: Not Applicable

Example:

```
MIBNav-> ctron
```

dir:

Syntax: dir [- 1pdm] [PATH]

Description: The dir command lists the contents of the directory sub-tree specified. If no [directory-path] is specified, the contents of the current directory are displayed. The display options are as follows:

-1 Displays the OID value along with the ASCII name of the leaf object.
-p Lists all the entries along with the path name of the leaf object.
-d Lists only the directory entries in the tree.
-m Displays one screen at a time.

Options: Not Applicable

Example:

```
MIBNav-> cd/iso/org/dod/internet
          dir
          mgmt
          private
          dir - lp
          /1/3/6/1/4/iso/org/dod/internet/private
```

get:

Syntax: get <PATH>

Description: The get command returns the value of a managed object. This is only valid for “leaf” entries in the MIB tree (or managed objects in the MIB).

Options: Not Applicable

Example:

```
MIBNav-> get /1/3/6/1/2/1/1/1
                #System name description
```

grep:

Syntax: grep <option> string

Description: Allows you to search the MIB tree for a specific character string. All leafs in the MIB tree are searched.

Options: -m Displays on the terminal one screen at a time.
-i Ignores case when searching for string.

Example:

```
MIBNav-> grep -i cabletron # /1/3/6/1/2/1/1/1 sysDescr String Cabletron MMAC-Plus Revision 01_01_01
```

ls:

Syntax: ls [-1pdm] [PATH]

Description: The ls command lists the contents of the directory sub-tree specified. If no [directory-path] is specified, the contents of the current directory are displayed. The display options are as follows:

-1 Displays the OID value along with the ASCII name of the leaf object.
-p Lists all the entries along with the path name of the leaf object.
-d Lists only the directory entries in the tree.
-m Displays one screen at a time.

Options: Not Applicable

Example:

```
MIBNav-> cd/iso/org/dod/internet
         ls - lp
         mgmt
         private
         ls - lp
         /1/3/6/1/2    /iso/org/dod/internet/mgmt
         /1/3/6/1/4    /iso/org/dod/internet/private
```

mib2:

Syntax: mib2

Description: The mib2 command allows you to move directly to the MIB II subtree (1.3.6.1.2.1) without entering the entire path.

Options: Not Applicable

Example:

```
MIBNav-> mib2
```

next:

Syntax: next [path]

Description: The next command enables you to determine the next leaf in the specified path within the managed device's MIB.

Options: Not Applicable

Example:

```
MIBNav-> next /1/3/6/1/2/1

#/1/3/6/1/2/1/1/1      sysDescr      String   CtronRev.X.XX.XX
```

pwd:

Syntax: pwd

Description: The pwd command displays the full pathname for the directory in which you are currently working. The directory is displayed in ASCII format.

Options: Not Applicable

Example:

```
MIBNav-> pwd

# /iso/org/dod/internet/mgmt/mib-2
```

set:

Syntax: set <OID> <value>

Description: The set command enables you to set the value of a managed object. This command is valid only for leaf entries in the current MIB tree, or for managed objects in the MIB.

If the leaf specified does not exist for the given path, MIB Navigator asks for a value. The following lists possible value types:

(i)nteger - number
(c)ounter - number
(g)auge - number
(t)ime ticks - number
o(p)aque - "value" (with quotation marks)
(s)tring - "value" (with quotation marks)
(o)id - OID number with dotted punctuation
(a)ddress - IP address in DDN format
(m)ac - MAC address in hexadecimal format
(n)ull - no type

Options: Not Applicable

Example:

```
MIBNav-> set /1/3/6/1/4/1/52/1/6/4/7 122.1.1.1

Type: (i)nteger (a)ddress (c)ounter (g)auge (o)id:
```

su:

Syntax: su [community name]

Description: The su command enables you to change your community name to allow for different access to the MIB. The community name that you enter allows you either read-only, read-write, or super-user access to that device's MIBs, depending on the level of security access assigned the password through the SNMP Community Names screen. Refer to the **SNMP Community Names Screen** section in **Chapter 1** for more information about community names.

Options: Not Applicable

Example:

```
MIBNav-> su public
```

tree:

Syntax: tree

Description: The tree command provides a display of the entire MIB for the device. Leaves and associated values are displayed in columns.

Options: Not Applicable

Example:

```
MIBNav-> tree

# /1/3/6/1/2/1/1/1   sysDescr      STRING       EMRev X.X.X.X
# /1/3/6/1/2/1/1/2   sysObjectId   OBJECT ID    1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3   sysUpTime     TIME TICKS   8098654
# /1/3/6/1/2/1/1/4   sysContact    STRING       AlZwie/MIS
```

wan:

Syntax: wan

Description: The wan command will change the current directory to Cabletron Systems WAN MIB: (/1/3/6/1/4/1/52/4/1/2/7/2).

Options: Not Applicable

whoami:

Syntax: whoami

Description: The whoami command displays your community string and access privileges to the MIB. When using the whoami command, one of these three access levels displays: read-only, read-write, and super-user.

Options: Not Applicable

Example:

```
MIBNav-> whoami

# Community Name      : super
# Access Level        : SuperUser
```

help:

Syntax: help <command>

Description: The help command provides general help on how to use the MIB Navigator or how to use a particular MIB Navigator command.

Options: A particular MIB Navigator command.

Example:

```
MIBNav-> help su

Command:        su
Format:         su <Community Name>
Allows user to change his/her community name, in
order to allow different access to the MIB.
```

PPP Security Command

The following is a command for PPP Security.

pppsecurity:

Syntax: pppsecurity <ifindex#><CHAP><direction><username><secret>

pppsecurity <ifindex#><PAP><direction><peerid><password>

pppsecurity <ifindex#><NONE>

Description: The pppsecurity command allows you to list and set PPP Security on an interface basis.

Options: Not Applicable

Example:

The example below shows the syntax used to set interface 7 to CHAP enabled.

```
MIBNav-> pppsecurity 7 "CHAP" 1 "localcyberswitch" "localsecurityword"
MIBNav-> pppsecurity 7 "CHAP" 2 "remotecyberswitch" "remotesecurityword"
```

Spoofing Command

The following is a command for Spoofing.

setspoof:

Syntax: setspoof <IF> <ON/OFF>
setspoof <IF> IPXRIP <TIME INTERVAL/ON/OFF>
setspoof <IF> IPXSAP <TIME INTERVAL/ON/OFF>
setspoof <IF> IPRIP <TIME INTERVAL/ON/OFF>
setspoof <IF> WDP <PACKETS COUNT/ON/OFF>
setspoof <IF> SPXWDP <PACKETS COUNT/ON/OFF>
setspoof <IF> NCPWAR <ON/OFF>
setspoof <IF> NCPMES <ON/OFF>

setspoof <IF> NB20 <ON/OFF>
setspoof <IF> SP <ON/OFF>

Description:The setspoof command allows the user to enable or disable spoofing on all the listed packet types or on a specific packet type. Where TIME INTERVAL: T=n*30(sec), where n belongs to the domain of natural numbers (1,2,3....), set spoofing on a time interval basis (in seconds); PACKETS COUNT: N - any natural number (except 1) Spoofs N packets, then allows the next packet through.
ON: enable spoofing
OFF: disable spoofing
Examples:
-> setspoof 4 on - will enable spoofing for all packet types on interface 4 using the default settings, unless enabled differently via a specific packet type.
-> setspoof 6 IPXSAP 1 - will enable IPX SAP spoofing on interface 6.
-> setspoof 8 IPXRIP 0 - will disable IPX RIP spoofing on interface 8.
-> setspoof 10 IPRIP 36000 - will spoof IP RIP on interface 10 on a 10 hour interval basis. (An IP RIP packet will be allowed through every 10 hours)
-> setspoof 4 WDP 40 - will spoof on a count of 40 watchdog packets on interface 4. (A WPD will be allowed through every 40 WDP packets)

Options: Not Applicable

Example:

The example below shows the syntax used.

```
MIBNav-> pppsecurity 7 "CHAP" 1 "localcyberswitch" "localsecurityword"
MIBNav-> pppsecurity 7 "CHAP" 2 "remotecyberswitch" "remotesecurityword"
```

ISDN Configuration Commands

The following ISDN configuration commands are used to set up primary and backup configurations.

setbackup:

Syntax: setbackup <PRIMARYIFNUM> <BACKUPIFNUM><TIMETOCONNECT> <TIMETODISCONNECT> <CONNECTRETRIESNUM> <TIMEBETWEENCONNECTRETRIES> <BACKUPOVERRIDE>

Description: The setbackup command allows you to configure backup/failover. Refer to **Configure Backup** in **Chapter 2** for more information.

Options: Not Applicable

Example:

```
MIBNav->  setbackup 7 8 35 45 10 15 no
-> setbackup 7 9 yes
Interface 9 will used to back up interface 7, backup override enabled,
other attributes remain unchanged.
-> setbackup 7 10
Interface 10 will used to back up interface 7, other attributes remain
unchanged.
```

setisdnbri:

Syntax: setisdnbri <WANPORTNUM> <LDN1> <SPID1> <LDN2> <SPID2>

Description: The setisdnbri command allows you to configure BRI.

Options: LDN1, SPID1, LDN2, and SPID2 can be skipped or cleared by entering S/s or C/c respectively. Trailing parameters do not have to be entered.

Example:

```
MIBNav-> setisdnbri 2 5554730 0555473001 5554732 0555473201
-> setisdnbri 2 s s c c
-> setisdnbri 2 s 0555473001
-> setisdnbri 2 5554730 0555473001
-> setisdnbri 2 c
-> setisdnbri 2 5554730 0555473001
```

setswitchtype:

Syntax: setswitchtype <WANPORTNUM> <SWITCHTYPE>

Description: The setswitchtype command allows you to set the switch type.

Options: Currently supported switch types are NI1 (BRI), ATT-5ESS (BRI/PRI), ATT-4ESS (PRI), DMS100 (BRI/PRI), and NET3 (BRI). Switch type is settable using one of the following: NI1, ATT5, ATT4, DMS100, or NET3.

Example:

```
MIBNav-> setswitchtype 1 ATT5
```

ct:

Syntax: ct <IFNUM>

Description: The ct command allows you to initiate the connection.

Options: Not Applicable

Example:

```
MIBNav-> ct 8
```

dt:

Syntax: dt <IFNUM>

Description: The dt command allows you to terminate the connection.

Options: Not Applicable

Example:

```
MIBNav-> dt 9
```

setidletimeout:

Syntax: setidletimeout <IFNUM> <TRANSMITIDLETIMEOUT> <RECEIVEIDLETIMEOUT>

Description: The setidletimeout command allows you to set the idle time out value in seconds in which a packet needs to be transmitted/received before the interface is automatically disconnected.

Options: Not Applicable

Example:

```
MIBNav-> setidletimeout 8  180  160
```

setalarmtime:

Syntax: setalarmtime <WANPORTNUM> <ALARMTIMEOUT>

Description: The setalarmtime command allows you to set the time out value in seconds in which the physical port must remain in a failed state to begin the backup procedure.

Options: Not Applicable

Example:

```
MIBNav-> setalarmtime 1  15
```

setmaxprofiles:

Syntax: setmaxprofiles <IFNUM> <MAXPROFILESNUM>

Description: The setmaxprofiles command allows you to set the maximum number of profiles for an interface.

Options: Not Applicable

Example:

```
MIBNav-> setmaxprofiles  8  16
```

setdemandif:

Syntax: setdemandif <DEMANDIFNUM> <TIMEBETWEENCONNECTRETRIES>

Description: The setdemandif command allows you to set the amount of time between retries to reconnect a primary demand interface which has failed.

Options: Not Applicable

Example:

```
MIBNav-> setdemandif  4  30
```

isdnstat:

Syntax: isdnstat <WANPORTNUM>
isdnstat callhist

Description: The isdnstat command allows you to list the ISDN settings and the Signalling channel status for a particular WANPORTNUM.
The callhist option shows the call history. The D channel status for NET3 switch type does not have to be active to place or receive a call. The inactive state is normal for this switch.

Options: Not Applicable

Example:

```
MIBNav-> isdnstat 1
```

ic:

This command is for Cabletron use only. Improper use may render an ISDN line unusable.

Other Commands

The other commands listed in this section activate functions on the LM managed device or devices being accessed through MIB Navigation.

arp:

Syntax: arp <options>

Description: The arp command provides access to the ARP (Address Resolution Protocol) cache, enabling you to view cache data, delete entries, or add a static route. Super-user access is required to delete an entry or add a static route.

Each ARP cache entry lists the network *interface* that the device is connected to, the device's *network address* or IP address, the device's *physical address* or MAC address, and the *media type* of connection to the device. Media types are displayed as numbers, which stand for the following states:

1 - Other
2 - Invalid entry (cannot ping device, timed out, etc.)
3 - Dynamic route entry
4 - Static route entry (not subject to change)

Options: -a Views cache data.
-d Deletes an IP address entry.
Requires additional arguments: <Interface Number> <IP address>
-s Adds a static entry.
Requires additional arguments: <Interface Number> <IP address> <MAC address>

Example:

```
MIBNav-> arp -a
# Interface          Network Address    Physical Address    Media Type
# (SonicInt)         122.144.40.111     00.00.0e.12.3c.04   3(dynamic)
# (SonicInt)         122.144.48.109     00.00.0e.f3.3d.14   3(dynamic)
# (SonicInt)         122.144.52.68      00.00.0e.12.3c.04   3(dynamic)
# (SonicInt)         122.144.21.43      00.00.0e.03.1d.3c   3(dynamic)

MIBNav-> arp -d 1 122.144.52.68

MIBNav-> arp -s 1 22.44.2.3 00:00:0e:03:1d:3c
```

051467

bridge:

Syntax: bridge <ENABLE/DISABLE> <IFNUM/ALL>

Description: The bridge command allows management of bridging upon one or more interfaces of the device. Bridging may be enabled or disabled at your request, either one at a time or all at once. Specifying a single interface number affects the bridging status of that interface, while specifying ALL affects every interface of the device.

Options: <ENABLE/DISABLE> Enables or disables bridging.

<IFNUM/ALL> Allows you to specify an interface number.

Example:

```
MIBNav-> bridge disable all
         bridge enable 1
         bridge disable 1
```

circuitmap:

Syntax: circuitmap -a <PROTOCOL>

circuitmap -f <PROTOCOL>

circuitmap -d <PROTOCOL> <INTERFACENUM> <NETADDRESS> <MACADDRESS>

circuitmap -s <PROTOCOL> <INTERFACENUM> <NETADDRESS> <MACADDRESS> <CIRCUIT>

Description: The circuitmap command allows you to view and/or modify a Protocol's Circuit Map (i.e., address-to-circuit) table for the device. The device must be initialized after changing the Circuit Map.

Options: -a Shows you the current Host Map information for the device.
-d Allows you to delete an entry from the table.
-s Allows you to insert a static entry into the table.
-f Allows you to flush the table.

Example:

```
MIBNav-> circuitmap -s IPX 2 00000172 00:00:1d:02:d1:7a 102
MIBNav-> circuitmap -a
# Interface      Network      Node              Circuit ID
  # 2            5A4C212B     00:00:1d:23:a1:5b 203
  # 2            00000172     00:00:1d:23:a1:5b 102
```

defroute:

Syntax: defroute [interface number] [IP address]

Description: The defroute command allows you to set the default IP route to a managed device through the specified interface.

Options: Not Applicable

Example:

```
MIBNav-> defroute 2 147.152.42.32
```

dhcp:

Syntax: dhcp <options>

Description: The dhcp command provides a status of the Dynamic Host Configuration Protocol feature. It allows you to enable/disable DHCP globally and by interface, and to configure interfaces with server parameters.

Options: dhcp (with no options) Displays DHCP status information.
dhcp enable/disable Enables or disables the DHCP feature globally.

dhcp <IFNUM> enable disable Enables or disables the DHCP feature by interface.

dhcp reclaim <IPADDRESS> Reclaims an IP address so another client can use it.

dhcp <IFNUM> <GATEWAY> <DNSADDRESS> <WINSADDRESS> <DOMAINNAME> The IFNUM is the Ethernet port number. The four configuration parameters can be passed to the hosts (clients). These are the IP address of their default gateway, the IP address of their domain name server, the IP address of their WINS server, and their domain name.

dhcp <IFNUM> <NETADDRESS> <NETMASK> <LOWADDRESS> <HIGHADDRESS> <LEASE> Allows you to specify the lease period for the hosts (clients), from one hour to many years. Selectable on a per port basis only.

<IFNUM> The Ethernet port number.

<NETADDRESS> The IP network on which the hosts will reside.

<NETMASK> The subnet mask for the hosts.

<LOWADDRESS> The lowest numerical value of the IP range to be allocated.

<HIGHADDRESS> The highest numerical value of the IP range.

Example:

```
MIBNav->dhcp
  DHCP Server Summary:
Admin: Enabled    Oper: Enabled    Server Time: 458400
Discovers: 0,   Offers: 0,   Requests: 2,   Errors: 0
Declines: 0,   Releases: 0,    Acks: 2,   Naks: 0,   Other Servers: 0

  DHCP Interface Configuration:
IF      Admin       Oper       ServerIP      Active     Free
 1    Enabled     Enabled   192.168.254.254    2       250
IF   Net Address        Net Mask          Low Address      High Address      Lease
 1   192.168.254.0     255.255.255.0   192.168.254.2    192.168.254.253   2880
IF   Default Gateway    DNS Address          WINS  Address     Domain Name
 1   192.168.254.254    134.141.72.219        134.141.70.34       ctron.com

  DHCP Client Status:
#    IF    MAC Address          Net Address       Time Left     Name

1     1    00:a0:c9:39:5e:40    192.168.254.2      22980        crotty
2     1    00:00:1d:16:71:99    192.168.254.3      22980        slowhand
```

ds1alarm:

Syntax:

ds1alarm
ds1alarm -ea <WANID>
ds1alarm -da <WANID>
ds1alarm -er <WANID>
ds1alarm -dr <WANID>
ds1alarm -et <WANID>
ds1alarm -dt <WANID>
ds1alarm -sec <WANID> <VALUE>
ds1alarm -sei <WANID> <VALUE>
ds1alarm -sbr <WANID> <VALUE>
ds1alarm -sbi <WANID> <VALUE>

Description:

The command “ds1alarm” with no options displays status information.

Options:

<WANID> Is either ALL to apply the command to all DS1 circuits, or it is the specific WAN physical identifier associated with the DS1 circuit.ds1alarm (with no options) displays status information.

ds1alarm -ea Enables the WAN DS1 Alarms Admin.
ds1alarm -da Disables the WAN DS1 Alarms Admin.
ds1alarm -er Enables the WAN DS1 Alarms Auto Recovery Feature.
ds1alarm -dr Disables the WAN DS1 Alarms Auto Recovery Feature.
ds1alarm -et Enables the WAN DS1 Alarms Traps Feature.
ds1alarm -dt Disables the WAN DS1 Alarms Traps Feature.
ds1alarm -sec Sets the Errored Seconds Threshold Count to VALUE.
ds1alarm -sei Sets the Errored Seconds Threshold Interval to VALUE.
ds1alarm -sbr Sets the Bipolar Violations Threshold Rate to VALUE.
ds1alarm -sbi Sets the Bipolar Violations Threshold Interval to VALUE.

fr:

Syntax: fr

Description: The fr command provides status related to Frame Relay and its Control Protocols. This allows you to monitor DLCIs and aids troubleshooting.

- MGR: This is the physical WPIM for the DLCI
- CKT: This is the virtual port number for the DLCI
- IF: This is the MIB II interface number for the DLCI
- DLCI: This is the circuit DLCI number
- DCP: This is the state of FR Data Compression on this DLCI (on/off)
- STATE: This is the DLCI circuit state (active/invalid/inactive)
- Inactive Reason: This value is empty for active/invalid states. It is filled in if the circuit is inactive. It has the following values:

  a. t391 Polling Error: This is a result of a failure in the Synchronous polling between us and the FR switch. If 3 out of any 4 polling cycles fail then both will place the link between us and the FR switch in a “link down” state. This will cause all DLCIs to be set to inactive, and no data placed on the wire (other than polling messages) until the service affecting condition is cleared. This service affecting condition can be the result of a number of things:

  - Our STATUS ENQUIRY message never reaches the FR switch, due to: our WAN driver, or our physical WAN connection to the Fr switch dropping the packet for some reason.
  - The STATUS RESPONSE message never reaches the FR protocol code, due to: our WAN driver, or our physical WAN connection to the Fr switch, or the FR switch itself dropping the packet for some reason.
  - The incorrect LMI type Si selected at our side or the Fr switch side. If they do not match, then polling errors will result.

b. DLCMI Protocol Error: This is a service affecting condition that can/will occur due to any error that has happened between/ before the link goes down due to excessive polling errors. If 3 out of 4 errors have not occurred yet, but the circuit was prevented from going active by any one of the FR errors listed in Section, then this will be the condition listed for the inactive reason.

c. Startup/Initialization: This basically means there have been no errors, we are polling correctly with the switch, but for some reason the switch reports to us inactive for that DLCI. Possible reasons for this are:

- The FR DTE bridge/router <-> FR DCE switch on the far side of the WAN cloud is not connected, or has polling error problems. Refer to the remote mibnav/LM screen for CSX products, the Telecommunications/Remote Access Service provider, or other means (remote device console support/ protocol analyzer) at the far end to troubleshoot the remote device.
- It may take up to 60 seconds (by default) [t391 (10 by default) seconds x n391 (6 by default) cycles for a circuit to go active, even in a well behaved properly communicating network. This is due to STATUS polling convergence of both FR DCE switches, with both FR DTE bridge/routers.

imux:

Syntax: imux <options>

Description: The imux command lets you balance your LAN traffic between two T1 WAN ports and is used with Point to Point Protocol (PPP). When you select Inverse Multiplexing via QuickSET, bridging, IP routing, and IPX routing functions are all disabled. The WAN device at the other end of the WAN link(s) must be a Cabletron Systems device, capable of receiving the balanced WAN traffic. The imux command with no options displays the status information.

Options:

-ea Enables the Inverse Multiplexer Application.
-da Disables the Inverse Multiplexer Application.
-eg <GROUPID> Enables the Inverse Multiplexer group designated by <GROUPID>.
-dg <GROUPID> Disables the Inverse Multiplexer group designated by <GROUPID>.
-ac <GROUPID> <INTERFACENUM> Adds the WAN channel designated by <INTERFACENUM> to the Inverse Multiplexer group designated by <GROUPID>.
-dc <GROUPID> <INTERFACENUM> Deletes the WAN channel designated by <INTERFACENUM> from the Inverse Multiplexer group designated by <GROUPID>.
<GROUPID> A unique value identifying an element in a sequence of groups that belong to the WAN Inverse Multiplexer Application.
<INTERFACENUM> The MIB II ifIndex value used to represent a WAN channel that has an appropriate datalink protocol associated with it.

Example:

```
MIBNav-> imux
WAN Inverse Multiplexer Status:
                                        WAN          Available BW    Xmit Byte Count
Group ID        Channel ID      Physical Number      (Kbits/sec)       (bytes)
-------------------------------------------------------------------------------
    1               1               1               1536000         291483387
    1               2               2               1536000         292249652
Number of WAN Inverse Multiplexer Groups currenly programmed: 1
Number of WAN Inverse Multiplexer Channels currenly programmed: 2
```

nat:

Syntax: nat <options>

Description: The nat command provides status relating to Network Address Translation. It allows you to assign a private network to an interface, to define an interface through which the internet can be accessed, and to create a public IP address to be used on the internet. It also allows you to assign a host on the private network as a “proxy server” accessible from the internet.

Options:

nat (with no options) Displays status information
nat enable/disable Enables or disables the NAT feature.
nat config <PRIVATEIFNUM> <PUBLICIFNUM> Selects the local and public interfaces.
nat proxy add <ENTRY_NUMBER> <PRIVATEIP> <PUBLICPORT> <LOCALPORT> <PROTOCOL> Adds a proxy server.
nat proxy delete <ENTRY_NUMBER> Deletes a proxy server.

Example:

```
MIBNav->nat
  NAT Status:
Admin: Enabled    Oper: Enabled    Local Interface: 1   Internet Interface: 2
Local IP          Local mask         Internet IP          Internet mask
192.168.254.254   255.255.255.0    134.141.17.165   255.255.0.0

Connections- TCP: 0, UDP: 0,  ICMP: 0

Local to inet- pkts: 116, bytes: 10814

Inet to local- pkts: 91, bytes: 39812

Errors: cksum: 0, retries: 1, bad packets: 0

Total IP pkts: 3917, Reserved addresses: 2919

 Server List:
Connections: #
# Number of valid entries: 0
```

netstat:

Syntax: netstat <option>

Description: The netstat command provides a display of general network statistics for the managed device. The netstat command must be used with one of the two display options.

Options: -i Displays status and capability information for each interface.
-r Displays routing information for each interface.

Example:

```
MIBNav-> netstat -i
Interface + Description     MTU     Speed      Admin  Oper  MAC Addr

# 1 (ethernet -csmacd)      1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x0e
# 2 (ethernet - csmacd)     1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x0f
# 3 (ethernet - csmacd)     1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x10
# 4 (ethernet - csmacd)     1514    10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x11

MIBNav-> netstat -r
Destination          Next-hop              Interface

# Default Route      DirectConnection      1
# 134.141.0.0        DirectConnection      2
# 134.141.0.0        DirectConnection      3
```

ping:

Syntax: ping [IP address]

Description: The ping command generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.

Options: Not Applicable

Example:

```
MIBNav-> ping 122.144.40.10

122.144.40.10 is alive
```

ppp:

Syntax: ppp

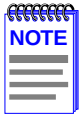
Description: The ppp command provides additional status relating to PPP and its Network Control Protocols.

Options: Not Applicable

reset:

Syntax: reset

Description: The reset command allows you to perform a soft reset of the device. You are queried to confirm the reset command to insure against unwanted resets.



The MIB Navigator's connection to the device is terminated upon execution of this command.

Options: Not Applicable

route:

Syntax: route add <IPADDRESS> <IPADDRESS> <INTERFACENUM>

route add <IPADDRESS> <IPADDRESS> <INTERFACENUM> <METRIC>

route delete <IPADDRESS> <IPADDRESS> <INTERFACENUM>

Description: The route command allows you to add or delete static entries in the IP Forwarding Table for the device. The first address is the destination. The second address is the next hop for the given interface. The metric value is optional. If included, it is used to set the value of **ipForwardingMetric1**. When RIP is used, the metric specifies the distance in hops to the destination.

secondIP:

Syntax: secondIP add <IPADDRESS> <INTERFACENUM>

secondIP delete <IPADDRESS> <INTERFACENUM>

Description: The secondIP command allows you to add or delete secondary IP addresses on the interface.

Options: Not Applicable

show:

Syntax: show <PROTOCOL> [TABLE]

Description: The show command displays information concerning various components of the device. Protocols currently supported are IP and IPX. Components of those protocols that are currently supported are ARP caches, route tables, FIB tables, server tables, interface tables, and events. The number of valid entries in the table is displayed at the end of the table.

Example:

```
MIBNav-> show IP ARP
# Interface    MediaType    Physical Address    NetworkAddress
# 4            (dynamic)    00:00:1d:04:40:5d   203
# 4            (dynamic)    08:00:20:0e:d8:31   102
```

snmpbranch:

Syntax: snmpbranch [IP address] [community name] [OID]

Description: The snmpbranch command enables you to query another SNMP device. The command provides a display of objects that match the specified OID. If no match is made, no object is displayed.

Options: Not Applicable

Example:

```
MIBNav-> snmpbranch 2.4.8.1 public 1.3.6.2.1.1

# /1/3/6/1/2/1/1/1   sysDescr      STRING       EMRev X.X.X.X
# /1/3/6/1/2/1/1/2   sysObjectId   OBJECT ID    1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3   sysUpTime     TIME TICKS   8098654
# /1/3/6/1/2/1/1/4   sysContact    STRING       AlZwie/MIS
```

snmpget:

Syntax: snmpget [IP address] [community name] [OID]

Description: The snmpget command enables you to query another SNMP device to obtain a value for a specified object. This command requires the appropriate community string and object id.

Options: Not Applicable

Example:

```
MIBNav-> snmpget 22.44.61.22 public 1.3.6.1.2.1.1.1.0

# Cabletron EMME Revision X.XX.XX
```

snmpnext:

Syntax: snmpnext [IPADDRESS] [COMMUNITY-STRING] [OBJECT-ID]

Description: The snmpnext command allows you to query another device using SNMP. The next leaf of an object identifier can be retrieved from that device by supplying an appropriate community string and the values of the object identifier.

Options: Not Applicable

Example:

```
MIBNav-> snmpnext 132.111.22.33 public 1.3.6.1.2.1.1.2
        #1.3.6.1.2.1.1.1.3 sysUpTime        Time Ticks  5490075
```

snmpset:

Syntax: snmpset [IP address] [community name]

Description: The snmpset command enables you to set the value of an object in other SNMP devices. This command requires the appropriate community string and OID.

When defining a new leaf set, MIB Navigator asks for a value. The following lists possible value types:

(i)nteger - number
(c)ounter - number
(g)auge - number
(t)ime ticks - number
o(p)aque - “value” (with quotation marks)
(s)tring - “value” (with quotation marks)
(o)id - OID number with dotted punctuation
(a)ddress - IP address in DDN format
(m)ac - MAC address in hexadecimal format
(n)ull - no type

Options: Not Applicable

Example:

```
MIBNav-> snmpset 122.44.1.2 public
        1.3.6.1.2.1.1.4.0 "Cyrus/MIS"
```

051475

snmptree:

Syntax: snmptree [IP address] [community name]

Description: The snmptree command provides a display of all objects in the device and their corresponding values.

Options: Not Applicable

Example:

```
MIBNav-> snmptree 122.144.89.10 public

# /1/3/6/1/2/1/1/1   sysDescr      STRING       EMRev X.X.X.X
# /1/3/6/1/2/1/1/2   sysObjectId   OBJECT ID    1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3   sysUpTime     TIME TICKS   8098654
# /1/3/6/1/2/1/1/4   sysContact    STRING       AlZwie/MIS
```

traceroute:

Syntax: traceroute [IP address]

Description: The traceroute command generates a TRACEROUTE request to a specified IP address and provides a display of all next-hop routers in the path to the device. If the device is not reached, the command displays all next-hop routers to the point of failure.

Options: Not Applicable

Example:

```
MIBNav-> traceroute 122.144.11.52

# next-hop[1]  122.144.61.45
# next-hop[2]  122.144.8.113
```

wanpq:

Syntax:

wanpq
wanpq -ea
wanpq -da
wanpq -aip <IPADDRESS>
wanpq -dip <IPADDRESS>

Description:

The wanpq command allows you to configure the WAN Priority Queue database. IPADDRESS is the Internet Protocol (IP) address being added to or removed from the Wide Area Network Priority Queue database.

Options:

wanpq (with no options) Displays status information.
wanpq -ea Enables the WAN Priority Queue Application.
wanpq -da Disables the WAN Priority Queue Application.
wanpq -aip <IPADDRESS> Adds the IP address designated by IPADDRESS to the WAN Priority Queue database.
wanpq -dip <IPADDRESS> Deletes the IP address designated by IPADDRESS from the WAN Priority Queue database.

Special Commands

done, quit, exit:

Syntax:

done
quit
exit

Description:

These commands enable you to exit from the MIB Navigator and return to the Main Menu screen.

Options:

Not Applicable

Example:

```
MIBNav-> done
```

A WPIM-SY Configuration

This Appendix explains how to configure the WPIM-SY in a PPP or Frame Relay environment through Local Management.

THE WAN PHYSICAL CONFIGURATION SCREEN

To access the WAN Physical Configuration screen from the Feature Selection screen, use the arrow keys to highlight the **WAN Configuration** option, then press ENTER. The screen shown in **Figure A-1** displays.

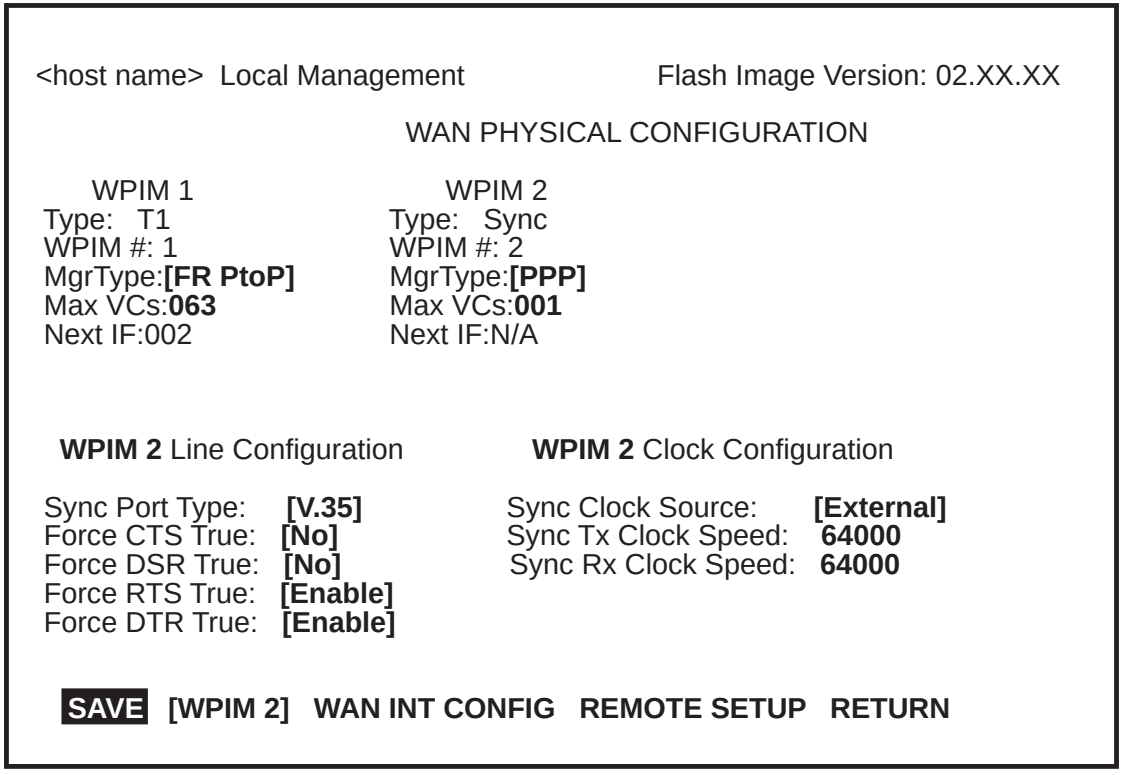


Figure A-1 WPIM-SY WAN Physical Configuration Screen

WPIM-SY Physical Configuration Fields

The configuration fields specific to the WPIM-SY shown in **Figure A-1** are defined as follows:

Sync Port Type — Displays the Synchronous port electrical interface type. The selections toggle between V.35, X.21, None, RS232, and RS422. This field always displays a Synchronous Port Type, even if the Synchronous Port is not the active WAN port. The default setting for this field is **V.35**.

Force CTS True — Displays the source of the Clear To Send (CTS) signal. The CTS signal is an input to the WPIM-SY. The WPIM-SY can either use or ignore the CTS signal. You can toggle the selections between Yes and No. The Yes (On) setting indicates that the WPIM-SY ignores the CTS signal from an external DCE (Data Communications Equipment) and forces the signal high. The No (Off) setting indicates that the CTS signal is received from an external DCE. The default setting is **No**.

Force DSR True — Displays the source of the Data Set Ready (DSR) signal. You can toggle the selections between Yes and No. The Yes (On) setting indicates that the DSR is internally "Forced True" . The No (Off) setting indicates that the DSR signal is received from an external DCE. The default setting is **No**.

Force RTS True — Displays the setting of the Ready To Send (RTS) signal. RTS Enable places the modem in the originate mode so it can begin to send. The default setting is Enable. The other choice is Disable. Used for sync modem backup. See **Appendix D**.

Force DTR True — Displays the setting of the Data Terminal Ready (DTR) signal. DTR Enable indicates that the DTE is powered on and ready to communicate. The default setting is Enable. The other choice is Disable. Used for sync modem backup. See **Appendix D**.

Sync Clock Source — Displays the clock source as External, Split, or Internal. The default setting is **External**. The Internal and Split settings are for Cabletron testing purposes only. Always set this field to External.

Sync Tx Clock Speed — Cabletron testing purposes only. Displays 64000 (Kbps) upon startup.

Sync Rx Clock Speed — This field displays the manually inputted receive clock speed. The default setting for this field is **64000** (Kbps). The information for this field is normally supplied by the Service Provider.

WAN Interface Configuration Screen Fields

Figure A-2 shows the WAN Interface Configuration screen fields specific to the WPIM-SY for PPP. Definitions of the fields are in **Chapter 2**.

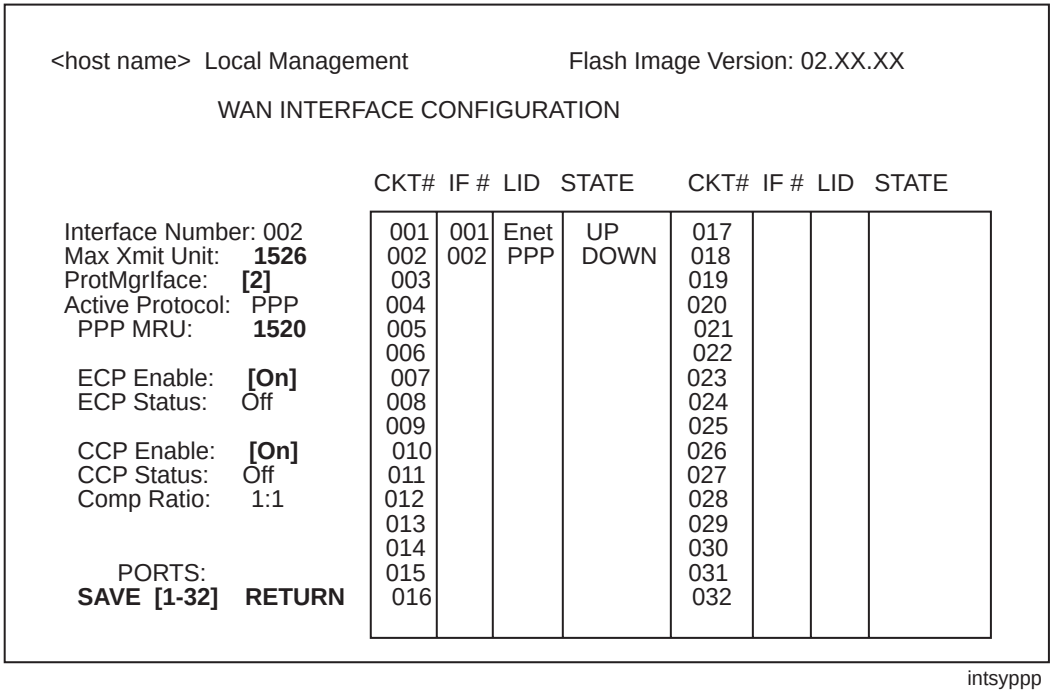


Figure A-2 WPIM-SY WAN Interface Configuration Screen

PPP CONFIGURATION

This section provides step-by-step instructions for connecting the WPIM-SY to a DDS (Digital Data System) circuit in a PPP environment. This example assumes the setup shown in **Figure A-3** using two WPIM-SY modules installed in each host platform.

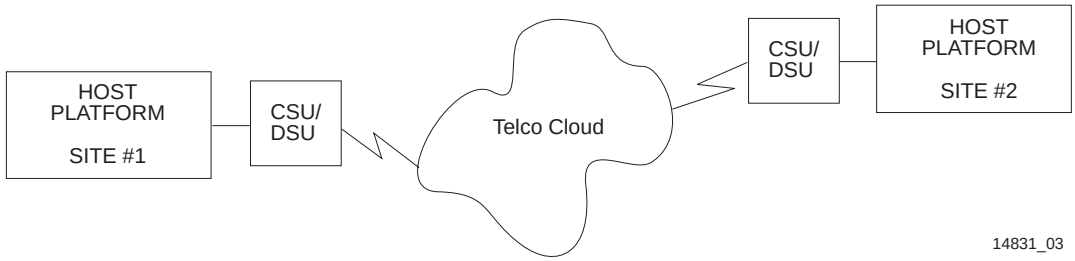


Figure A-3 WPIM-SY Interface Configuration for PPP

The line configuration information shown in **Table A-1** must be supplied by the service provider.

Table A-1 Telco Configuration Information

Configuration Information Required By User	Configuration Information Supplied By Service Provider
Clock Source	Telco provided or no clock source
Circuit Speed	64K, V.35, RS-422, RS-232, etc.

WPIM-SY Physical Configuration

Begin the WPIM-SY configuration by accessing the WAN Configuration screen through Local Management (**Figure A-1**). Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM]** field at the bottom of the screen. Press the SPACEBAR to select the WPIM-SY.
2. Use the arrow keys to highlight **Mgr Type**. Press the SPACE bar to set the Mgr Type to **PPP**.
3. Use the arrow keys to highlight **SYNC PORT TYPE**. Press the SPACE bar to set the Sync Port Type to V.35, RS422, RS232, None, or X.21.
4. Use the arrow keys to highlight **FORCE CTS True**. Press the SPACE bar to set to **NO**.
5. Use the arrow keys to highlight **FORCE DSR True**. Press the SPACE bar to set to **NO**.

6. Use the arrow keys to highlight **FORCE RTS True**. Press the SPACE bar to set to **ENABLE**.
7. Use the arrow keys to highlight **FORCE DTR True**. Press the SPACE bar to set to **ENABLE**.

Set **FORCE CTS** and **FORCE DSR** to YES only if the CSU/DSU does not support these flow control terms.

8. Use the arrow keys to highlight the **SAVE** command. Then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory and the device reboots. Local Management must be reaccessed before any other configurations may be made.
9. Proceed to the next section for the WPIM-SY Interface Configuration.

WPIM-SY Interface Configuration

This screen is accessed through the WAN Physical Configuration screen. Refer to **Figure A-2** and proceed with the following steps to configure the WAN Interface through Local Management.

1. Access the WAN Interface Configuration screen by using the arrow keys to highlight the **WAN Int Config** option, then press ENTER.
2. Use the arrow keys to highlight **Interface Number**. Set the WAN connection Interface Number by typing the same number found in the Interfaces field on the WAN Physical Configuration screen into the Interface Number field, or use the SPACE bar to toggle to the correct Interface Number, then press ENTER.
3. Use the arrow keys to highlight **ECP Enable**. Press the SPACEBAR to select **On** to enable encryption.
4. Use the arrow keys to highlight **CCP Enable**. Press the SPACEBAR to select **On** to enable compression.
5. Make any other changes as desired.
6. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory.

The WAN configuration is complete. It takes up to 60 seconds for the WAN Interface to come out of standby and for communications to begin.

FRAME RELAY CONFIGURATION

This section provides instructions for connecting the WPIM-SY to a DDS (Digital Data System) circuit in a Frame Relay environment. Refer back to **Figure A-3** for the configuration.

The line configuration information shown in **Table A-1** must be supplied by the service provider.

Table A-2 Telco Configuration Information

Configuration Information Required By User	Configuration Information Supplied By Service Provider
Clock Source	Telco provided or no clock source
Circuit Speed	64K, V.35, RS-422, RS-232, etc.

WPIM-SY Physical Configuration

Begin the WPIM-SY Frame Relay configuration by accessing the WAN Configuration screen through Local Management. Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM]** field at the bottom of the screen. Press the SPACEBAR to select the WPIM being configured, then press ENTER.
2. Use the arrow keys to highlight **Mgr Type**. Press the SPACEBAR to set the Mgr Type to FR PtoMP (Frame Relay Point to Multipoint) or FR PtoP (Frame Relay Point to Point), then press ENTER. These are the two settings for Frame Relay. Frame Relay Point to Point has one Interface per DLCI assigned when DLCIs are created by the Service Provider. In Frame Relay Point to Multipoint, there is one interface to multiple DLCI'S, and the DLCIs are dynamically learned. Backup can only be run on FR PtoP, not FR PtoMP.
3. Use the arrow keys to highlight **SYNC PORT TYPE**. Press the SPACEBAR to set the Sync Port Type to V.35, RS422, RS232, or X.21.
4. Use the arrow keys to highlight **FORCE CTS True**. Press the SPACEBAR to set to **NO**.
5. Use the arrow keys to highlight **FORCE DSR True**. Press the SPACEBAR to set to **NO**.
6. Use the arrow keys to highlight **FORCE RTS True**. Press the SPACEBAR to set to **ENABLE**.
7. Use the arrow keys to highlight **FORCE DTR True**. Press the SPACEBAR to set to **ENABLE**.

Set **FORCE CTS** and **FORCE DSR** to YES only if the CSU/DSU does not support these flow control terms.

8. Use the arrow keys to highlight the **SAVE** command. Then press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory and the device reboots. Local Management must be re-entered for any further configuration.

WPIM-SY Interface Configuration

For Frame Relay, this screen is only accessed to configure FR LMI. Refer to **Figure A-4** and proceed with the following steps.

1. Access the WAN Interface Configuration screen by using the arrow keys to highlight the **WAN Int Config** option, then press ENTER.
2. Use the arrow keys to highlight **ProtMgrIface**. Choose the interface to be configured.
3. Use the arrow keys to highlight **FR LMI**. Press the SPACE bar to choose from ANSI 94, No LMI, T1.617-D, or Q.933-A, then press ENTER.

The choice No LMI under FR LMI is a test mode only and must not be used in a practical application.

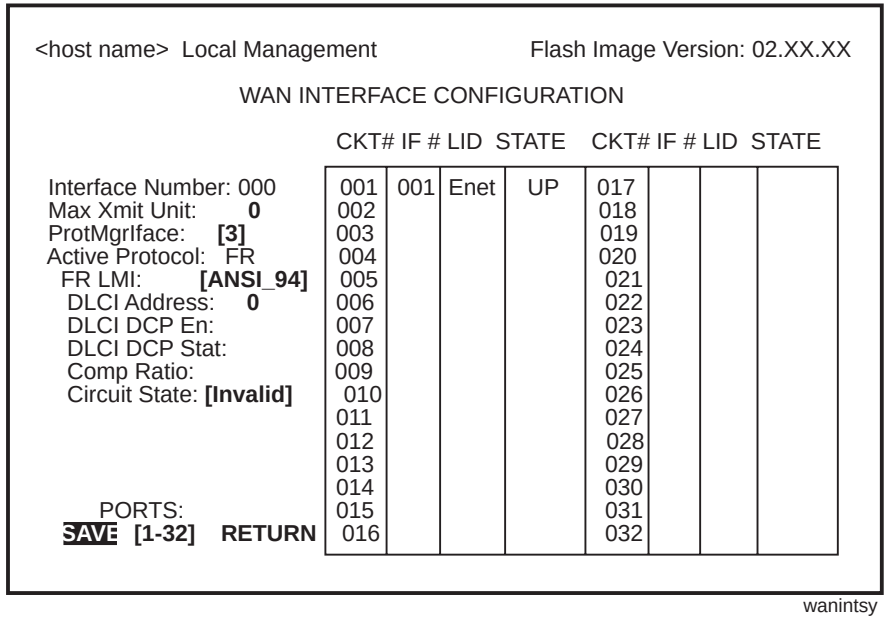


Figure A-4 WPIM-SY WAN Interface Configuration Screen

4. Make any other changes as desired.

5. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory.

The WAN configuration is complete. Communications between the WPIM-SY and the service provider’s switch takes approximately 1 to 2 minutes to begin. A status of **Inactive** displays until both ends of the PVC (Permanent Virtual Circuit) are configured. Once both end devices have negotiated link management with the switches, the status field reads **Active**.

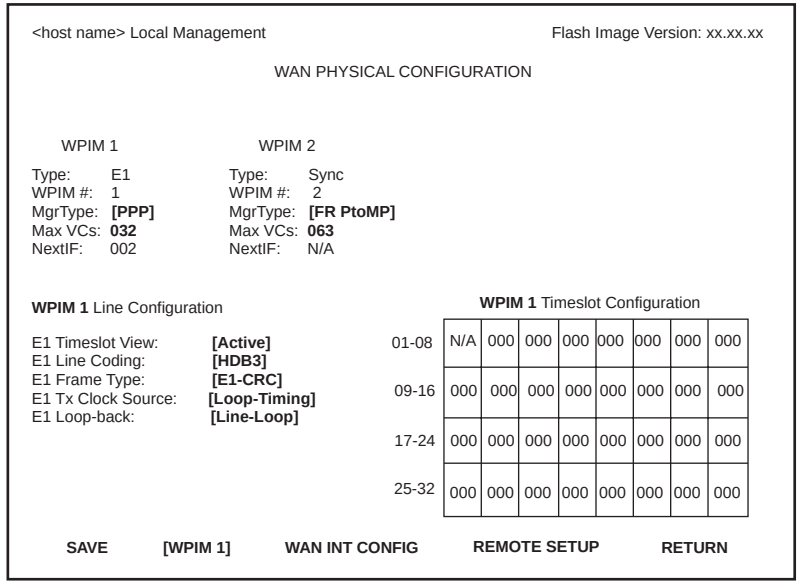
B WPIM-E1 Configuration

This Appendix explains how to configure the WPIM-E1 through Local Management. Sections of this chapter include:

- Full T-1 Configuration Using PPP
- Fractional T-1 Configuration Using PPP
- Frame Relay Configuration

THE WAN PHYSICAL CONFIGURATION SCREEN

To access the WAN Physical Configuration screen from the Feature Selection screen, use the arrow keys to highlight the WAN Configuration option, then press ENTER. The screen shown in **Figure B-1** displays.



1484_01

Figure B-1 WAN Physical Configuration Screen

WPIM-E1 Configuration Fields

The WPIM1 configuration fields displayed on the Physical Configuration screen in **Figure B-1** are specific to the WPIM-E1.

The service provider determines the settings for the following fields. Consult the service provider for the correct settings.

E1 Timeslot View — Displays the status of the Timeslot Configuration Table. The selections for this field toggle between Active and New. The Active setting displays current Timeslot Configuration table settings. The default setting is **Active**. The New setting allows you to change Timeslot Configuration table settings. The default setting for the Timeslot Configuration table is all timeslots not assigned (**000**).

E1 Line Coding — Displays the line coding for the physical E1 line. The selections toggle between HDB3 and AMI. The default setting for this field is **HDB3**.

E1 Frame Type — Displays the E1 Frame type. The selections toggle between E1 and E1-CRC. The default setting for this field is **E1-CRC**.

E1 Tx Clock Source — Displays the E1 Transmit Clock Source. The selections for this field toggle between Loop-Timing (Extracted Line Data) and Local-Timing (Internal Clock). The default setting for this field is **Loop-Timing**.

E1 Loop-back — Network Loop-back is a testing procedure that segments the line and allows the user to isolate faults. It is not used during normal operation. The selections for this field toggle between None and Line-Loop. In Line-Loop all 32 channels are looped back to the E1 line.The WPIM-E1 must be in Loop-Timing mode to use this option. The default setting is **None**.

The WPIM Timeslot Configuration Table

The WPIM Timeslot Configuration Table allows the user to configure the way in which the Cabletron WAN module uses the E1 line. The configuration table consists of 32 timeslots. Only 31 of the timeslots are available for use, because the first timeslot is used by the device to transmit framing data. **N/A** (Not Available) always displays in Timeslot #1. You must assign each of the remaining 31 timeslots an **Interface** number (for example, 002 for an active Interface number or 000 if the timeslot is not used). When you lease an entire E1 line, you can use all 31 timeslots (the full E1 bandwidth). If you lease only a fraction of the E1, the service provider tells you which timeslots to use.

The WPIM-E1 always uses the first timeslot (Timeslot #1) to transmit framing data. A full E1 line with 32 timeslots has 31 customer-usable timeslots.

You can utilize timeslots any way you choose. The WPIM-E1 supports Time Division Multiplexing (TDM) allowing demultiplexing of circuits (timeslots) within the public network. For example, if you have access to a full E1 (31 customer-usable timeslots), and you want to communicate with two other sites, your configuration might look like **Figure B-2**.

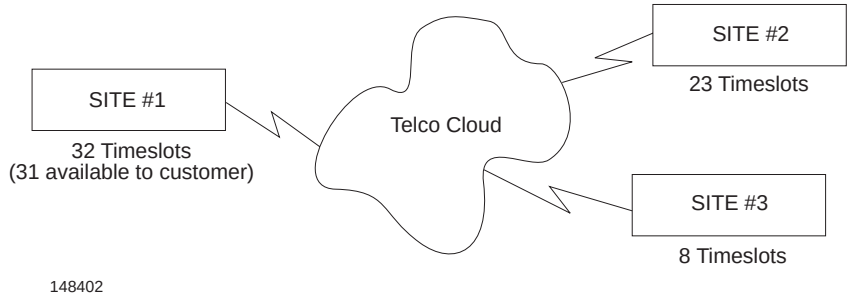


Figure B-2 Sample Timeslot Configuration

Figure B-3 shows a sample configuration for three sites. Of the 32 timeslots, Site #1 uses the first timeslot for transmitting framing data, 23 timeslots to communicate with Site #2 and the remaining 8 timeslots to communicate with Site #3. This configuration varies tremendously depending on how the service provider maps out the E1 timeslots. Your service provider will tell you which timeslots to configure.

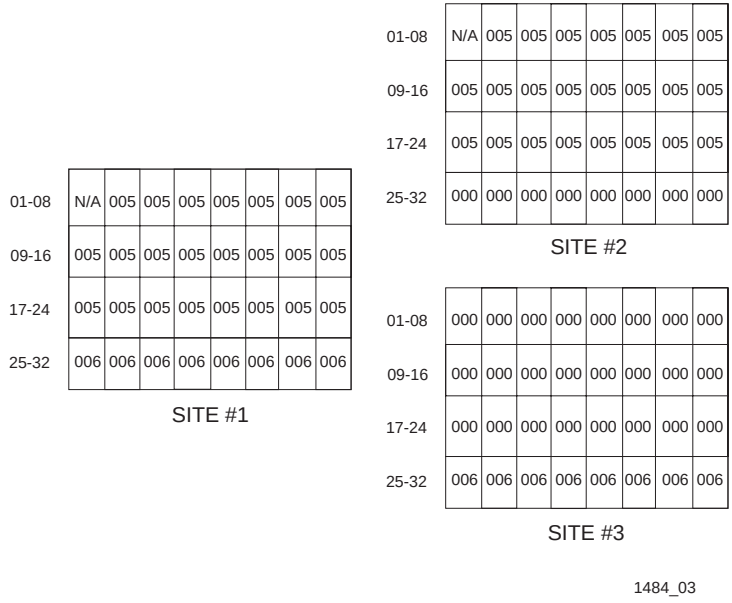


Figure B-3 Sample Configuration

Site #1 is using the full E1, so all the timeslots must have an Interface assignment. Site #2 and Site #3 only use a fraction of the E1, but the total quantity of timeslots assigned must match those of Site #1. Unused timeslots receive an Interface number of 000.

The Interface numbers of Site #1, Site #2 and Site #3 do not have to match. Only the **quantity** of timeslots must match (the service provider assigns the timeslots).

THE WAN INTERFACE CONFIGURATION SCREEN

Figure B-4 displays the WAN Interface Configuration screen specific to the WPIM-E1 in PPP mode.

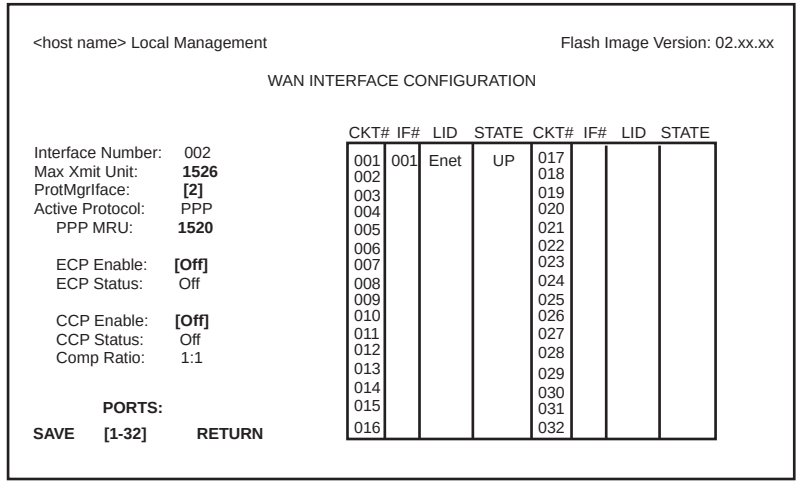

<host name> Local Management
Flash Image Version: 02.xx.xx
WAN INTERFACE CONFIGURATION
Interface Number: 002
Max Xmit Unit: 1526
ProtMgrIface: [2]
Active Protocol: PPP
PPP MRU: 1520
ECP Enable: [Off]
ECP Status: Off
CCP Enable: [Off]
CCP Status: Off
Comp Ratio: 1:1
PORTS:
SAVE [1-32] RETURN
CKT# IF# LID STATE CKT# IF# LID STATE
001 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016
001 Enet UP
017 018 019 020 021 022 023 024 025 026 027 028 029 030 031 032
1484_04

Figure B-4 WAN Interface Configuration Screen

FULL E1 CONFIGURATION USING PPP

This section provides step-by-step instructions for configuring the WPIM-E1 to use a full E1 circuit in a PPP environment. This simplified example assumes the setup shown in **Figure B-5** using a host platform containing a WPIM-E1 at Site #1. Configurations may vary depending on the host platform.

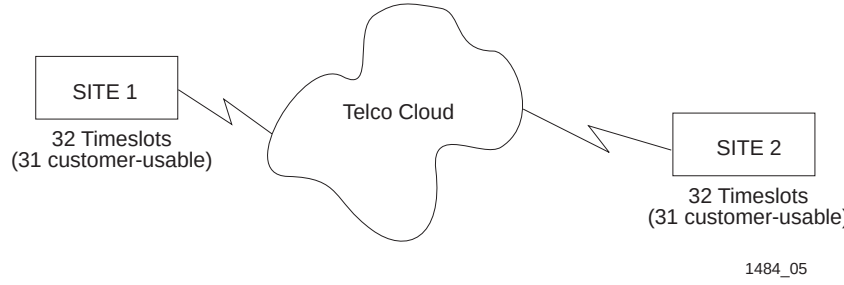


Figure B-5 Full E1 Configuration

The line configuration information shown in **Table B-1** must be supplied by the service provider.

Table B-1 Telco Configuration Information

Configuration Information Required By User	Configuration Information Supplied By Service Provider
Line Coding	HDB3 or AMI
Frame Type	E1 or E1-CRC
Clock Source	Loop Timing or Local Timing

WPIM-E1 Physical Configuration

Begin the WPIM-E1 configuration by accessing the WAN Physical Configuration screen through Local Management (**Figure B-1**). Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM]** field at the bottom of the screen. Press the SPACEBAR to select the WPIM being configured, then press ENTER.
2. Use the arrow keys to highlight the **MgrType**. Press the SPACE bar to select PPP, then press ENTER.
3. Use the arrow keys to highlight **Timeslot View**. Press the SPACEBAR to select **New**, then press ENTER. The cursor moves to Timeslot #2 of the Timeslot Configuration Table.
4. Insert an interface number (see NOTE below) into every timeslot. Type the number, press ENTER, then use the arrow keys to highlight the next timeslot field. Exit this field by using the arrow keys. The cursor automatically moves to the **E1 Line Coding** field.

The value assigned to the timeslots is the interface being used for WAN communication. The next available interface is displayed on the WAN Physical Configuration screen (see **Figure B-1**).

The following three steps are based on information supplied by the service provider. Consult the service provider for the correct settings.

5. Use the arrow keys to highlight **E1 Line Coding**. Press the SPACEBAR to select **HDB3** or **AMI**.
6. Use the arrow keys to highlight **E1 Frame Type**. Press the SPACEBAR to select **E1** or **E1-CRC**.

7. Use the arrow keys to highlight **E1 Tx Clock Source**. Press the SPACEBAR to select **Local** (no clock source provided by telephone company) or **Loop** (clock source provided by telephone company).

If you are using a Local clock source, set only one end of the circuit for Local, the other end must be set for Loop.

8. Use the arrow keys to highlight **E1 Network Loopback.** Press the SPACEBAR to select **None**.
9. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory and the host platform reboots. Local Management must be reaccessed before any other configurations may be made.

WPIM-E1 Interface Configuration

This screen is accessed through the WAN Physical Configuration screen. Refer to **Figure B-4** and proceed with the following steps to configure the WAN Interface through Local Management.

1. Access the WAN Interface Configuration screen by using the arrow keys to highlight the **WAN Int Config** option, then press ENTER.
2. If the correct Interface number to be configured is not displayed, enter it by typing the number into the **Interface Number** field or select it using the SPACE bar, then press ENTER (see note on **page B-6**).
3. Unless the user sets the Max Xmit Unit, the WPIM-E1 automatically sets the **Max Xmit Unit** to **8191** (default) after the active protocol (PPP) is selected.
4. Configure other settings, including ECP and CCP, as desired.
5. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory.

The WAN configuration is complete. It takes up to 60 seconds for the WAN Interface to come out of standby and for communications to begin.

FRACTIONAL E1 CONFIGURATION USING PPP

This section provides step-by-step instructions for configuring the WPIM-E1 to use a fractional E1 circuit in a PPP environment. This example assumes the setup shown in **Figure B-6** using two host platforms, each containing a WPIM-E1. In a fractional E1 setup, only a portion of the 32 timeslots or DS-0's are used.

NOTE

The terms DS-0 (Digital Signal, level 0) and timeslot are used synonymously in this guide to represent a standard 64,000 bit/second channel.

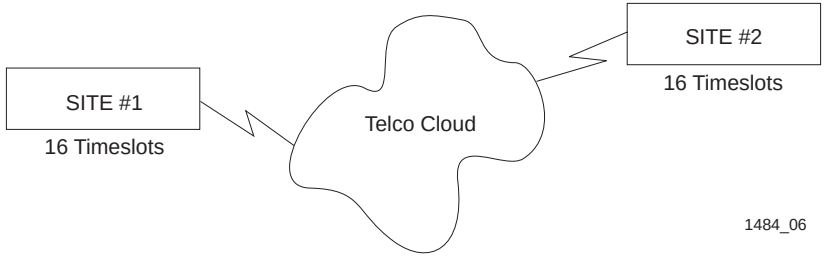


Figure B-6 Fractional E1 Configuration

The line configuration information shown in **Table B-2** must be supplied by the service provider.

Table B-2 Telco Configuration Information

Configuration Information Required By User	Configuration Information Supplied By Service Provider
Line Coding	HDB3 or AMI
Frame Type	E1 or E1-CRC
Clock Source	Loop Timing or Local Timing
DS-0's (Timeslots)	Timeslots being used for each end of the circuit

WPIM-E1 Physical Configuration

Begin the WPIM-E1 configuration by accessing the WAN Physical Configuration screen through Local Management (**Figure B-1**). Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM]** field at the bottom of the screen. Press the SPACEBAR to toggle the field to the WPIM being configured, then press ENTER.
2. Use the arrow keys to highlight the **MgrType**. Press the SPACE bar to select PPP, then press ENTER.
3. Use the arrow keys to highlight **Timeslot View**. Press the SPACEBAR to select **New**, then press ENTER. The cursor moves to Timeslot #2 of the Timeslot Configuration Table.
4. Insert an interface number (see NOTE below) into every timeslot being used (in the example shown in **Figure B-6**, 16 timeslots are being used, the rest have zeros in them). Type the number, press ENTER, then use the arrow keys to highlight the next timeslot field. Exit this field by using the arrow keys.The cursor automatically moves to the **E1 Line Coding** field.

The value assigned to the timeslots is the interface being used for WAN communication. The next available interface is displayed on the WAN Physical Configuration screen (see **Figure B-1**).

The following three steps are based on information supplied by the service provider. Consult the service provider for the correct settings.

5. Use the arrow keys to highlight **E1 Line Coding**. Press the SPACEBAR to select **HDB3** or **AMI**.
6. Use the arrow keys to highlight **E1 Frame Type**. Press the SPACEBAR to select **E1** or **E1-CRC**.
7. Use the arrow keys to highlight **E1 Tx Clock Source**. Press the SPACEBAR to select **Local** (no clock source provided by telephone company) or **Loop** (clock source provided by telephone company).

If you are using a Local clock source, set only one end of the circuit for Local, the other end must be set for Loop.

8. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory. The host platform reboots. For further configuration, the Local Management connection must be re-accessed.

WPIM-E1 Interface Configuration

This screen is accessed from the WAN Physical Configuration screen. Proceed with the following steps to configure the WAN Interface through Local Management.

1. Access the WAN Interface Configuration screen by using the arrow keys to highlight the **WAN Int Config** option and then press ENTER.
2. If the correct Interface number to be configured is not displayed, enter it by typing the number into the **Interface Number** field or select it using the SPACE bar, then press ENTER (see note on **page B-6**).
3. Unless the user sets the Max Xmit Unit, the WPIM-E1 automatically sets the **Max Xmit Unit** to **8191** (default) after the active protocol (PPP) is selected.
4. Configure other settings, including ECP and CCP, as desired.
5. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message “Save Done!” displays and Local Management saves the changes to memory.

The WAN configuration is complete. It takes up to 60 seconds for the WAN Interface to come out of standby and for communications to begin.

FRAME RELAY CONFIGURATION

This section provides step-by-step instructions for configuring the WPIM-E1 to use an E1 circuit in a Frame Relay environment. This example assumes the setup shown in **Figure B-7**, using two host platforms each containing a WPIM-E1. Configurations may vary depending on the host platform.

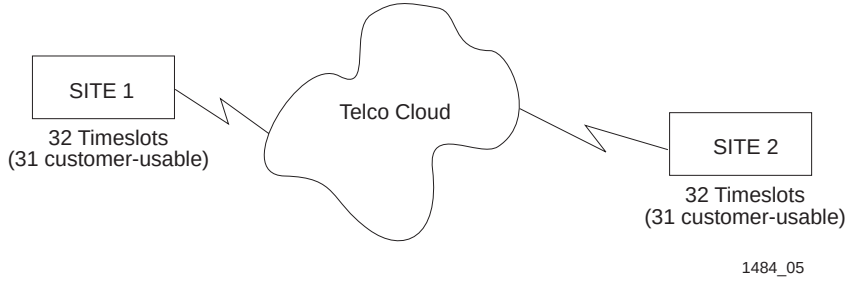


Figure B-7 Frame Relay Configuration

The following information must be supplied to the service provider.

- LMI type: **Q.933-A**

The line configuration information shown in **Table B-3** must be supplied by the service provider.

Table B-3 Telco Configuration Information

Configuration Information Required By Customer	Information Supplied By Service Provider
Line Coding	HDB3 or AMI
Frame Type	E1 or E1-CRC
Clock Source	Loop Timing or Local Timing
DSO's (Timeslots)	Timeslots being used for each end of the circuit

WPIM-E1 Physical Configuration

Begin the WPIM-E1 configuration by accessing the WAN Physical Configuration screen through Local Management (**Figure B-1**). Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM]** field at the bottom of the screen. Press the SPACEBAR to select the WPIM being configured, then press ENTER.
2. Use the arrow keys to highlight the MgrType. Select either FR Pto MP (Frame Relay Point to Multipoint) or FR PtoP (Frame Relay Point to Point) using the SPACE bar.
3. Use the arrow keys to highlight **Timeslot View**. Press the SPACEBAR to select **New**, then press ENTER. The cursor moves to Timeslot #2 of the Timeslot Configuration Table.
4. Insert an interface number (see NOTE on **page B-6**) into every timeslot being used. Type the number, press ENTER, then use the arrow keys to highlight the next timeslot field. Exit this field by using the arrow keys. The cursor automatically moves to the **E1 Line Coding** field.
5. Use the arrow keys to highlight **E1 Line Coding**. Press the SPACEBAR to select **HDB3** or **AMI**.
6. Use the arrow keys to highlight **E1 Frame Type**. Press the SPACEBAR to select **E1** or **E1-CRC**.
7. Use the arrow keys to highlight **E1 Tx Clock Source**. Press the SPACEBAR to select **Local** (no clock source provided by telephone company) or **Loop** (clock source provided by telephone company).

If you are using a Local clock source, set only one end of the circuit for Local, the other end must be set for Loop.

8. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory. The host platform reboots. For further configuration, the Local Management connection must be re-accessed.

WPIM-E1 Interface Configuration

This screen is accessed through the WAN Physical Configuration screen. Proceed with the following steps to configure the WAN Interface through Local Management.

1. Access the WAN Interface Configuration screen by using the arrow keys to highlight the **WAN Int Config** option and then press ENTER.
2. If the correct Interface number to be configured is not displayed, enter it by typing the number into the **Interface Number** field or select it using the SPACE bar, then press ENTER (see note on **page B-6**).
3. Use the arrow keys to highlight **Line Coding**. Press the SPACEBAR to select **None**.
4. Use the arrow keys to highlight **Active Protocol**. Press the SPACEBAR to select **FR**.
5. Use the arrow keys to highlight **FR LMI**. Press the SPACEBAR to select **Q.933-A**.
6. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory.

Upon saving this screen, the interface just configured is assigned to an application port (CKT#) in the table on the right hand side of the screen once the device starts communicating with the service provider's switch.

The WAN configuration is complete. Communications between the WPIM-E1 and the service provider's switch takes approximately 1-2 minutes to begin. A status of **Inactive** displays until both ends of the PVC (Permanent Virtual Circuit) are configured. Once both end devices have negotiated link management with the switches, the status field reads **Active**.

C WPIM-DI Configuration

This chapter explains how to configure the WPIM-DI through Local Management. It provides instructions for setting up the WPIM-DI for full or fractional T-1 in a PPP environment, or for configuring the WPIM-DI for Frame Relay.

The WAN Physical Configuration Screen

To access the WAN Physical Configuration screen from the Setup Menu screen, use the arrow keys to highlight the **WAN Setup** option, then press ENTER. The screen shown in **Figure C-1** displays.

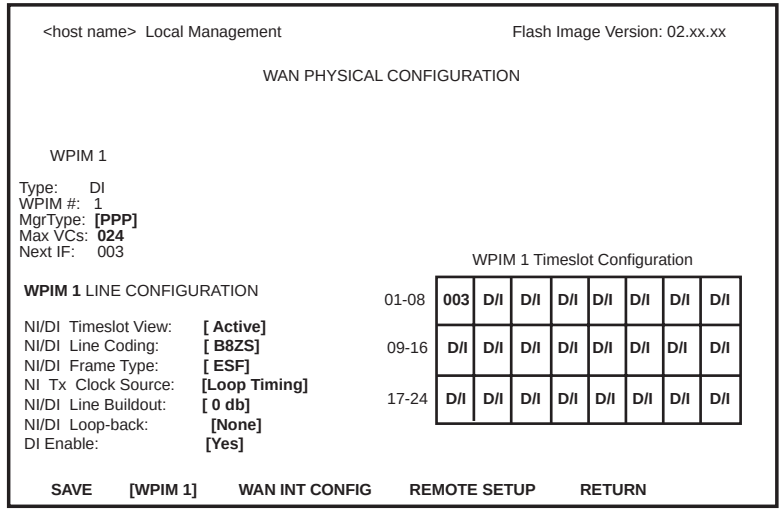

<host name> Local Management
Flash Image Version: 02.xx.xx
WAN PHYSICAL CONFIGURATION
WPIM 1
Type: DI
WPIM #: 1
MgrType: [PPP]
Max VCs: 024
Next IF: 003
WPIM 1 Timeslot Configuration
01-08 003 D/I D/I D/I D/I D/I D/I D/I
09-16 D/I D/I D/I D/I D/I D/I D/I D/I
17-24 D/I D/I D/I D/I D/I D/I D/I D/I
WPIM 1 LINE CONFIGURATION
NI/DI Timeslot View: [Active]
NI/DI Line Coding: [B8ZS]
NI/DI Frame Type: [ESF]
NI Tx Clock Source: [Loop Timing]
NI/DI Line Buildout: [0 db]
NI/DI Loop-back: [None]
DI Enable: [Yes]
SAVE [WPIM 1] WAN INT CONFIG REMOTE SETUP RETURN
1482_01

Figure C-1 WAN Physical Configuration Screen

WPIM-DI Line Configuration Fields

NOTE

The service provider (i.e., AT&T, Sprint, MCI, NYNEX, etc.) determines the settings for the following fields. Consult the service provider for the correct settings.

NI/DI Timeslot View — Displays the status of the Timeslot Configuration table. This field toggles between Active and New. The Active setting displays current Timeslot Configuration table settings. The New setting allows you to change Timeslot Configuration table settings. The default setting is **Active** (D/I).

NI/DI Line Coding — Displays the line coding for the physical T-1 line. This field toggles between B8ZS and AMI. The default setting is **B8ZS**.

NI/DI Frame Type — Displays the T-1 Frame type. This field toggles between ESF and D4. The default setting is **ESF**.

NI/DI Tx Clock Source — Displays the T-1 Transmit Clock Source. This field toggles between Loop Timing (Extracted Line Data) and Local Timing (Internal Clock). The default setting is **Loop Timing**. If the DI Enabled field is set to diDataEnable, Local Timing cannot be selected as a choice.

NI/DI Line Buildout — Displays the line coding for the physical T-1 line. Set this field to 0 dB unless the service provider recommends another setting. The default setting is **0 dB**. This field steps between the following levels:

- 0 db
- -7.5 db
- -15 db
- -22.5 db

NI/DI Loop-back — Displays the loopback for the WPIM-DI. Loopback is a testing procedure that segments the line and allows the user to isolate faults. This field toggles between None, Line-Loop, and Payload-Loop. In Line-Loop the entire T1 is looped back. In Payload-Loop only the 24 timeslots are looped back. The NI/DI Tx Clock Source must be in Loop Timing mode to use this option. The default setting is **None**.

DI Enable — Displays the status of the Drop-and-Insert function of the WPIM-DI. This field steps between On, Off, and diDataEnable. Choosing **On** allows another device (e.g., WPIM-T1) that is connected to the DI interface of the WPIM-DI to use any timeslots that the WPIM-DI is not using (Drop and Insert is enabled between the two ports). The data from the host device passes through the NI port. Choosing **Off** allows the Network Interface to be used as a standard T-1 port. Choosing **diDataEnable** enables Drop and Insert, and data from the host device will pass through the DI port. The default setting is **On**.

NOTE

When the **diDataEnable** option is selected in the DI Enabled field, data from the host device passes through the DI port and not the NI port on the host platform.

WPIM-DI Timeslot Configuration Table

The WPIM Timeslot Configuration table allows you to configure the way in which the WAN module uses the T-1 line. The configuration table consists of 24 timeslots. You must assign each timeslot an Interface number (for example, 002 for an active Interface number or 000 if the timeslot is not used). When you lease an entire T-1 line, you can use all 24 timeslots (the full T-1 bandwidth). If you lease only a fraction of the T-1, the service provider tells you which timeslots to use.

The WPIM-DI supports Time Division Multiplexing (TDM) allowing channelization of circuits (Timeslots) within the public network. You can use timeslots any way you choose. When using the WPIM-DI, you have the option of implementing all the available leased timeslots with the WPIM-DI, or you may map any of the available timeslots to another WAN module through the DI interface.

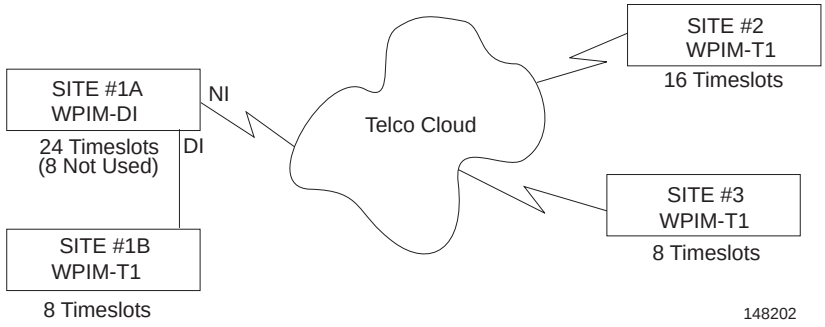


Figure C-2 Sample Network Configuration

Figure C-3 shows a sample timeslot configuration for the network shown in **Figure C-2**. Of the 24 timeslots, the WPIM-DI at Site #1A uses 16 to communicate with Site #2 and the remaining 8 are mapped to the WPIM-T1 at Site #1B. The WPIM-T1 at Site #1B uses these to communicate with Site #3. This configuration varies tremendously depending on how the service provider maps out the T-1 timeslots. Your service provider will tell you which timeslots are active.

Figure C-3 Sample Timeslot Configuration

Site #1 is using the full T-1, so all the timeslots must have an Interface assignment. Site #2 and Site #3 only use a fraction of the T-1, but the total quantity of timeslots must match those of Site #1. Unused timeslots receive an Interface number of 000.

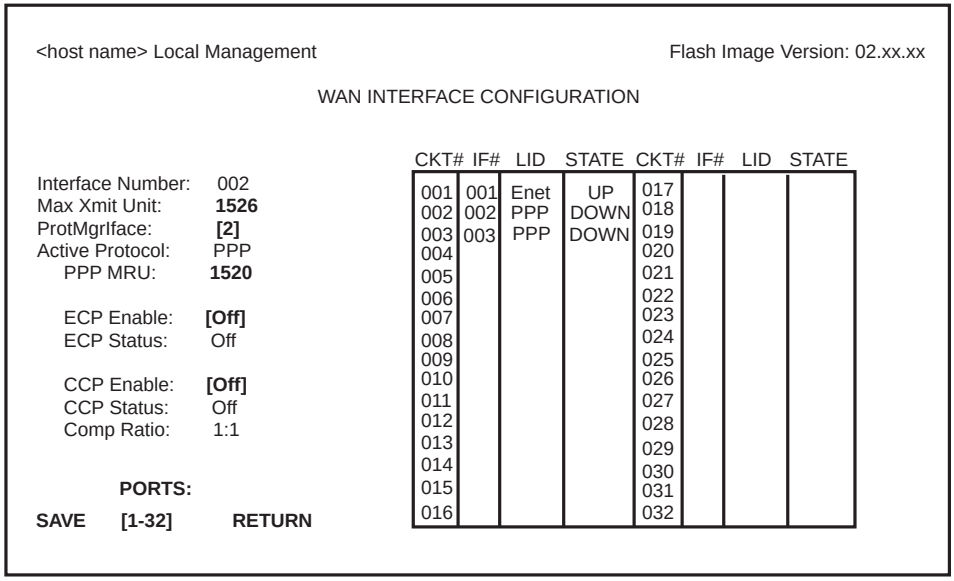
NOTE

When the Drop-and-Insert function is enabled, and the WPIM-DI Physical Configuration screen is saved, the timeslots will display “DI” to reflect that these timeslots are mapped to the DI interface. If the Drop-and-Insert function is disabled, the timeslots will display “000” in the Timeslot Configuration table when the screen is saved.

In order to map unused timeslots to another device connected to the DI port of the WPIM-DI, the DI Enable option on the WAN Physical Configuration screen must be set to **On**.

The WAN Interface Configuration Screen

This section describes the features of the WAN Interface Configuration screen. Access the screen by using the arrow keys to highlight the **WAN INT CONFIG** option at the bottom of the Physical Configuration screen, then press ENTER. The WAN Interface Configuration screen shown in **Figure C-4** displays.



148401_04

Figure C-4 WAN Interface Configuration Screen

WPIM-DI Configuration

This section provides step-by-step instructions for configuring the WPIM-DI to use a full or fractional T-1 circuit in a PPP or Frame Relay environment. This simplified example assumes the setup shown in **Figure C-5** using two host platforms containing a WPIM-DI at Site #1 and a WPIM-T1 at Site #2. Configurations may vary depending on the host platform.

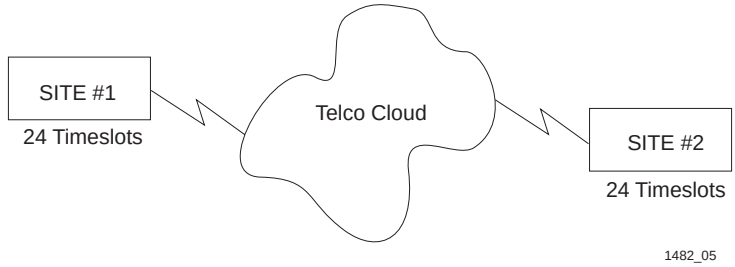


Figure C-5 Full T-1 Configuration

The line configuration information shown in **Table C-1** must be supplied by the service provider.

Table C-1 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
Line Coding	B8ZS or AMI
Frame Type	ESF or D4
Clock Source	Loop Timing or Local Timing
DS0 (Timeslots)	Timeslots being used for each end of the circuit

WPIM-DI Physical Configuration

Begin the configuration by accessing the WAN Physical Configuration screen (**Figure C-1**) through Local Management. Proceed with the following steps:

1. Use the arrow keys to highlight the **[WPIM]** field at the bottom of the screen. Press the SPACE bar to select the WPIM being configured, then press ENTER.
2. Use the arrow keys to highlight the **MgrType** field. Press the SPACE bar to choose the desired Protocol Manager.

3. Use the arrow keys to highlight **NI/DI Timeslot View**. Press the SPACE bar to select **New**, then press ENTER. The cursor moves to Timeslot #1 of the Timeslot Configuration table.
4. Insert an interface number (refer to the NOTE on **page C-7**) into every Timeslot. Type the number, press ENTER, then use the arrow keys to highlight the next timeslot field. Exit this field by using the arrow keys. The cursor automatically moves to the **NI/DI Line Coding** field.

NOTES

The value assigned to the timeslots is the interface being used for WAN communication. The available interface range is displayed on the WAN Physical Configuration screen (see **Figure C-1**). You may insert any of the available interface numbers into the timeslots.

Any timeslots that are given a value of 000 are either not used (DI Enabled set to Off) or are mapped to another WAN module (e.g., WPIM-T1) that is connected to the DI interface (DI Enabled set to On).

When DI Enabled is set to diDataEnable, the timeslot view changes to view data from DI. Host data passes through the DI interface and slots that are marked DI are mapped to the NI interface.

The following four steps are based on information supplied by the service provider. Consult the service provider for the correct settings.

5. Use the arrow keys to highlight **NI/DI Line Coding**. Press the SPACE bar to select **B8ZS** or **AMI**.
6. Use the arrow keys to highlight **NI/DI Frame Type**. Press the SPACE bar to select **ESF** or **D4**.
7. Use the arrow keys to highlight **NI Tx Clock Source**. Press the SPACE bar to select **Local Timing** (no clock source provided by telephone company) or **Loop Timing** (clock source provided by telephone company).

NOTE

If you are using a Local clock source, set only one end of the circuit for Local Timing, the other end must be set for Loop Timing.

8. Use the arrow keys to highlight **NI/DI Line Buildout** (LBO). Press the SPACE bar to select **0 db** unless the service provider recommends another setting.
9. Use the arrow keys to highlight **NI/DI Loop-back**. Press the SPACE bar to select **None**.

10. Use the arrow keys to highlight **DI Enable**. Press the SPACE bar to select **On** (Drop and Insert function enabled), or **Off** (Drop and Insert function disabled), or **diDataEnable** (Drop and Insert is enabled and the data that comes to the host goes to the DI port).
11. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory. The host device reboots. For further configuration, Local Management must be re-accessed.

WPIM-DI Interface Configuration

This screen is accessed from the WAN Physical Configuration screen. Refer to **Figure C-4** and proceed with the following steps to configure the WAN Interface through Local Management.

1. Access the WAN Interface Configuration screen by using the arrow keys to highlight the **WAN INT CONFIG** option, then press ENTER.
2. If the correct Interface number to be configured is not displayed, enter it by typing the number into the **Interface Number** field or select it using the SPACE bar, then press ENTER.
3. Unless the user sets the Max Xmit Unit, the WPIM-DI automatically sets the **Max Xmit Unit** to the default after the active protocol (PPP or FR) is selected.
4. If you selected **FR** as the Protocol Manager, use the arrow keys to highlight **FR LMI**. Press the SPACE bar to select **T1.617-D**, then press ENTER.
5. Make any other configurations as needed, such as ECP or CCP.
6. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The message "Save Done!" displays and Local Management saves the changes to memory.

Upon saving this screen, the interface just configured is assigned to an application port (CKT#) in the table on the right hand side of the screen.

The WAN configuration is complete. It takes up to 60 seconds for the WAN Interface to come out of standby and for communications to begin.

D Modem Settings for RS-232 Dial-up PPP Backup

This appendix details the backup configuration of a Frame Relay or PPP nailed-up connection using modems and the WPIM-SY.

TIP

To avoid incurring a cost due to possible unintentional call(s) do not connect the modem line to the telephone wall jack until both the modem and the host platform have been configured.

The modem used in the first example is the FastPro II (GDC 060R124-000) from General DataComm. The second example uses the Courier B.Everything from USRobotics (3COM). Any brand modem meeting these requirements may be used. A typical configuration can be seen in **Figure D-1**.

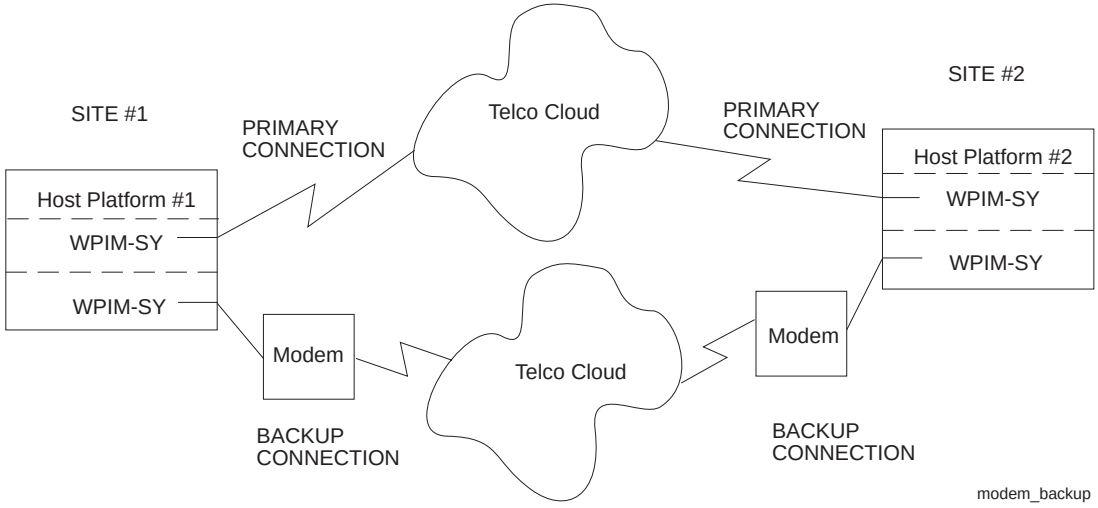


Figure D-1 Originate (Caller/Backup-side) Modem Configuration

FastPro-II Modem Configuration

Origination Modem Configuration

The caller side must be configured for the following:

- DTR off to on transition causes modem to automatically dial previously stored phone number.
- Data mode of operation set to call is placed using the asynchronous call establishment command set. Once the call connection is established, switch to synchronous mode for transmission.
- DSR follows/tracks CD.

In all of the following tables, each command is preceded by the AT keyword. For example, AT&C1.

Use the Extended AT(tention) command set listed in the following table to configure the modem:

Command	Action
&C1	Carrier on after link established (normally the default setting).
&D2	Enables automatic dialing. When: DTR on - go off hook (place call). DTR off - go on hook (hang-up).
&M1	Selects asynchronous command mode/synchronous data mode.
&R1	Selects Real synchronous mode, Real asynchronous mode, and AT command mode (normally the default setting).
&S2	Sets DSR to follow Carrier Detect (CD).
%Z1	Enables automatic dialing when DTR off-to-on.
&Z1=nnn	Store the specified remote phone number, including any dial command modifiers. e.g., the area code in user configuration profile number 1. Up to nine digits can be entered, i.e., n= 0 to 9.
&Y1	Selects user configuration profile #1 to load as the default profile at power-up.
&W1	Save the above settings as user configuration profile number 1.

Command	Action
&$	List the AT& command set settings to verify the configuration.
%$	List the AT% command set settings to verify the configuration.

To verify that the settings have been saved, power down the modem, power it back up, enter the AT&$ command, and then the AT% command.

Answer Side Modem Configuration

The answer side must be configured for the following:

- Ignore DTR state.
- Normal DSR operation.

Using the Extended AT(tention) command set listed in the following table to configure the modem:

Command	Action
&C1	Carrier on after link established (normally the default setting).
&D0	Ignore DTR state (normally the default setting).
&M1	Selects asynchronous command mode/synchronous data mode.
&R1	Selects Real synchronous mode, Real asynchronous mode, and AT command mode (normally the default setting).
&S1	DSR normal operation (normally the default setting).
&Y1	Selects user configuration profile #1 to load as the default profile at power-up.
&W1	Save the above settings as user configuration profile number 1.
&$	List the AT& command set settings to verify the configuration.

To verify that the settings have been saved, power down the modem, then power it up again and enter the AT&$ command.

For the CSX-400: if DTR and RTS are not enabled, force DTR and RTS on (ENABLED) under the corresponding PPP-SYNC WPIM via the WAN setup screen. Normally this is the default setting.

Courier V.Everything Modem Configuration

Originate (Caller/backup) Side Modem Configuration

The caller side must be configured for the following:

- DTR off to on transition causes modem to automatically dial previously stored phone number.
- Data mode of operation set to call placed using the asynchronous call establishment command set. Once the call connection is established switch to synchronous mode for transmission.
- DSR follows/tracks CD.

Use the Extended AT(tention) command set to configure the modem. Assume the default on all settings that are not specified, including DIP switch settings. Use the following list to perform the configuration:

Command	Action
DT	The default dialing service setting is pulse. If your dialing service is tone, this command is set to dial the backup site phone number using tone dial.
&C1	Carrier on after link established (normally the default setting).
&D2	Normal DTR operations. Normally the default setting.
&M1	Selects asynchronous command mode/synchronous data mode.
&R2	Send data to the DTE device on receipt of RTS (normally the default setting). Same as h/w flow control enabled.
&S4	Simultaneous DSR and CD.
S13=8	Bit 3 on. Enables automatic dialing when DTR off-to-on transition. Auto dials the number stored in NVRAM at position 0, same as profile zero.
&Z0=nnn	Store the specified remote phone number including any dial command modifiers, such as the area code in user configuration profile number 1. Up to nine digits can be entered (n= 0 to 9).
&W	Save the above settings.
I5	List the current NVRAM settings to verify the configuration.
I4	List the current non-NVRAM settings to verify the configuration.

To verify that the settings have been saved, power down the modem, power it back up, enter the ATI5 command, then the ATI4 command.

Answer Side Modem Configuration

The answer side must be configured for the following:

- Normal DTR operations.
- Normal CD operations.
- Simultaneous DSR and CD.

Use the Extended AT(tention) command set to configure the modem. Assume the default on all settings not specified, including DIP switch settings.

Use the following list to perform the configuration:

Command	Action
DT	The default dialing service setting is pulse. If your dialing service is tone this command will set to dial the backup site phone number using tone dial.
&C1	Carrier on after link established (normally the default setting).
&D2	Normal DTR operations. Normally the default setting.
&M1	Selects asynchronous command mode/synchronous data mode.
&R2	Send data to the DTE device on receipt of RTS (normally the default setting). Same as h/w flow control enabled.
&S4	Simultaneous DSR and CD.
&W	Save the above settings.
I5	List the current NVRAM settings to verify the configuration.
I4	List the current non-NVRAM settings to verify the configuration.

To verify that the settings have indeed been saved, power down the modem, power it back up, enter the ATI5 command, then the ATI4 command.

DIP Switch setting: Set DIP switch number five OFF for Auto answer.

For the CSX-400: if DTR and RTS are not enabled, force DTR and RTS on (ENABLED) under the corresponding PPP-SYNC WPIM via the WAN setup screen. Normally this is the default setting.

E Glossary

10BASE-T — IEEE 802.3 standard for the use of Ethernet LAN technology over Unshielded Twisted Pair wiring, running at 10 Mbps.

ARP — Address Resolution Protocol. An Internet protocol used to bind an IP address to Ethernet/802.3 addresses.

ASCII — American Standard Code for Information Interchange. It is an 8-bit code for character representation.

AUI — Attachment Unit Interface. An IEEE 802.3 transceiver cable connecting the network device (such as a router) to the MAU (media access unit).

Bandwidth on Demand — Feature providing the capability of adjusting the bandwidth (opening or closing multiple B channels) when the load in traffic increases or decreases.

Bridge — A device that segments network traffic. A bridge maintains a list of each node on the segment and only traffic destined for a node on the adjacent segment is passed across the bridge. A bridge operates at Layer 2 of the OSI reference model.

B Channel — In ISDN, a full-duplex, 64 Kbps channel used for sending user data.

BRI — Basic Rate Interface. The ISDN interface providing two 64 Kbps B channels for voice, data and video transmission and one 16 Kbps D channel for signaling and data transmission.

CHAP — Challenge Handshake Authentication Protocol. A security protocol supported under point-to-point protocol (PPP) used to prevent unauthorized access to devices and remote networks. Uses encryption of password, device names and random number generation.

DCE — Data Communications Equipment. Equipment used within a network to transfer data from source to destination such as modems.

D Channel — In ISDN, a full-duplex 16 Kbps channel used for link setup.

Data Compression — Techniques used to reduce the number of bits transferred across the communication links that represent the actual data bits. Compression is used to optimize use of WAN links and speed data transmission.

DHCP — Dynamic Host Configuration Protocol is a protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.

Dial on Demand — Dial up WAN resources are accessed only when remote access is required and released as soon as the resource is no longer needed.

DTE — Data Terminating Equipment. DTE refers to equipment used in a network as the data source and/or destination, such as computers.

DTMF — Dual Tone Multi-Frequency. TOUCHTONE as opposed to Dial Pulse (DP).

DTR — Data Terminal Ready. RS232 signal used for indicating to the DCE the readiness to transmit and receive data.

EtherTalk — AppleTalk protocols running on Ethernet.

Filter — Feature to control the flow of data based on protocol or bridge information. Filters can be specific to allow data through or prevent transmission.

Firewall — A combination of techniques used to protect one network from unknown networks and users on the outside. Firewalls can filter or block traffic and act as a management and network security point where all traffic can be scrutinized.

Frame — A group of data generated by Data Link Layer operation.

Frame Relay — Data Link Protocol that provides connectivity between one local and numerous remote connections.

HDSL — High bit rate Digital Subscriber Line. A technology to put two-way T1 on a normal unshielded, bridged (but not loaded) twisted pair without using repeaters.

IMUX (Inverse Multiplexing) — The process of splitting a single high-speed channel into multiple signals, transmitting the multiple signals over multiple facilities operating at a lower rate than the original signal, and then recombining the separately-transmitted portions into the original signal at the original rate.

In-Band Signaling — Transmission within the frequency range used for data transmission; i.e., results in use of bandwidth normally reserved for data.

IP — Internet protocol. A network layer protocol which allows a packet to traverse multiple networks on the way to its final destination.

IP Address — Internet address. A 32-bit address assigned to devices that participate in a network using TCP/IP. An IP address consists of four octets separated with periods defining network, optional subnet and host sections.

IPX (Internet Packet Exchange) — A proprietary Network layer protocol developed by Novell and used in NetWare networks.

ISDN — Integrated Services Digital Network. Digital transmission standard defining communication protocols permitting telephone networks to carry data, voice, fax and other streams.

Leased Line — A telecommunications line between two service points leased from a communications carrier for private use, usually incurring a monthly service rate.

LEDs (Light Emitting Diodes) — Type of indicator lights on the panel of a device.

Local Area Network (LAN) — A network connecting computers over a relatively small geographic area (usually within a single campus or building).

MAC Layer/Address — Media Access Control layer/address defined by the IEEE 802.3 specification which defines media access including framing and error detection. Part of the OSI reference model Data Link layer.

Metric — An algorithm used by routers to determine the best path for transmitting packets to a remote destination based on considerations such as time, delay, cost, etc.

Modem — Modulator/Demodulator. A device that converts digital signals to/from analog signals for transmission over analog communications lines.

Multi-Link Protocol — A protocol, defined in RFC 1717, that defines a way to perform inverse multiplexing on the TCP/IP point-to-point protocol (PPP); i.e., the ability to use multiple serial WAN channels for transferring one datastream. With MLP, a user can send and receive data over both B channels in an ISDN basic-rate interface connection

NAT — Network Address Translation uses a unique IP address for a WAN interface. This IP Address is negotiated through PPP or assigned statically by the Internet Service Provider (ISP). NAT reduces the number of unique IP addresses for all clients using a particular WAN interface to one.

NetWare — A Network Operating System developed by Novell, Inc. providing shared access to files and other network services.

Network Layer — Layer 3 of the OSI reference model that provides the protocol routing function.

Node — Refers to a termination point for communication links; entity that can access a network.

OSI — Open System Interconnection. An international standard developed by ITU (formally CCITT) and ISO (International Organization for Standardization) to facilitate data networking multi-vendor interoperability. The OSI Reference Model defines seven layers, each providing specific network functions.

Packet — A group of data that includes a header and usually user data for transmission through a network.

Ping (Packet Internet Groper) — An echo message, available within the TCP/IP protocol suite, sent to a remote node and returned; used to test the accessibility of the remote node.

PPP (Point-to-Point Protocol) — A Data Link layer protocol that provides asynchronous and synchronous connectivity between computer/network nodes. Includes standardization for security and compression negotiation.

Q.921 — ISDN Data Link layer specification for the user-to-network interface.

Q.931 — ISDN specification for call set-up and signaling on ISDN connections.

Q.933 — ITU Frame Relay Data Link Layer specification for UNI.

RFC — Request for Comment. Documentation describing Internet communications specifications (e.g., Telnet, TFTP). Often these RFCs are used to achieve multi-vendor interoperability during implementation.

RJ11 — Standard 4-wire connectors for telephone lines.

RJ45 — Standard 8-wire connectors used for ISDN lines and 10 BASE-T connections.

RIP (Routing Information Protocol) — Protocols used in IP and IPX for broadcasting open path information between routers to keep routing tables current.

Routing — A Network layer function that determines the path for transmitting packets through a network from source to destination.

RS-232 — EIA standard specifying the physical layer interface used to connect a device to communications media.

Serialization Frames — Frames sent out by servers under IPX to check whether illegal copies of NetWare are in use on the network.

Service Advertising Protocol — Protocol used in IPX for broadcasting information about services available on the network, such as file servers, CD-ROM drives and modem pools.

SNMP — Simple Network Management Protocol. A widely implemented Internet network management protocol that allows status monitoring, getting/setting of parameters for configuration and control of network devices, such as routers and bridges.

Split B Channels — Each 64 Kbps ISDN B-channel can be used individually for a separate data connection.

Spoofing — Spoofing is a technique used to remove poll and update service frames from WAN links while ensuring that the network continues to operate normally. Spoofing is employed to minimize dial-up line connection time.

Subnet Address — An extension of the Internet 32-bit addressing scheme that allows the separation of physical or logical networks within the single network number assigned to an organization. TCP/IP entities outside this organization have no knowledge of the internal "subnetting."

Subnet Mask — A 32-bit internet protocol address mask used to identify a particular subnetwork.

T1.617 — ANSI Frame Relay Data Link Layer specification for UNI.

TCP/IP — Transmission Control Protocol/Internet Protocol. Refers to a set of internetworking protocols developed by the U.S. Department of Defense that define a two level layered approach for interoperability. TCP provides a connection-oriented Transport layer ensuring end-to-end reliability in data transmission. IP provides for Network layer connectivity using connectionless datagrams.

Telco Cloud — The "cloud" of switched virtual connections over a Wide Area Network (WAN).

TELNET — Internet standard protocol for remote terminal emulation that allows a user to remotely log in to another device and appear as if directly connected.

TFTP — Trivial File Transfer Protocol. A simplified version of the File Transfer Protocol (FTP) allowing for file transfer between computers over a network.

Transparent Bridging — Bridging technique used in Ethernet networks that allows transfer of frames across intermediate nodes using tables associating end nodes with bridging addresses. Bridges are unknown to the end nodes.

UDP — User Datagram Protocol. A connectionless protocol used to pass packets across an internet network, requiring no handshaking between source and destination.

Watchdog Frames — Frames sent out by servers to clients, under IPX, to verify that clients are still logged on.

Wide Area Network — A communications network that is geographically dispersed thus requiring links provided by communications carriers.

Workstation — Computer or terminal used by the systems administration or user.

Index

B

Backup
    Modem settings D-1
Bootstrap Protocol Client 1-38
Bootstrap Protocol Server 1-38
Bridge Setup
    bridge port pair administrative status 1-31
    port administrative status 1-30
    spanning tree protocol 1-29
Broadcast 1-40

C

Call Backup
    ISDN 1-3
Call Backup Topology 1-4
Configuring the Network Broadcast Type on a port 1-40
Configuring the UDP Broadcast Redirector 1-38

D

Default Gateway 1-17, 1-19
Default Interface 1-17, 1-20
Domain Name Server 1-38

E

Enabling Forwarding on a port
    IP 1-38, 1-52
Enabling Proxy ARP on a port 1-39
Enabling Routing Services on a port
    IP 1-37, 1-52
Enabling the RIP Routing Protocol on a port 1-40, 1-55

F

Flash Download
    bootprom 1-26, 1-28
    runtime 1-27

H

Host IP Address 1-16, 1-19
Host Name Server 1-38

I

IP
    Configuring the Network Broadcast Type on a port 1-40
    Configuring the UDP Broadcast Redirector 1-38
    Enabling Forwarding on a port 1-38, 1-52
    Enabling Proxy ARP on a port 1-39
    Enabling Routing Services on a port 1-37
    Enabling the RIP Routing Protocol on a port 1-40, 1-55
    Selecting a port for configuration 1-36, 1-50
IPX
    enabling forwarding on a port 1-52
    enabling RIP on a port 1-55
    enabling routing services on a port 1-52
    enabling SAP on a port 1-54
ISDN 1-3

K

Keyboard conventions 1-8

L

Local Management
    exiting screens 1-10
    navigating menu screens 1-13
    selecting menu screen items 1-12

WAN Interface Configuration screen 2-10, A-3, C-5
WAN Physical Configuration screen 2-2, 2-3, 2-30, A-1, B-1, C-1
Local Management Screen Fields
command fields 1-7
display fields 1-7
event message field 1-7
input fields 1-7
selection fields 1-7

M

Management Agent 1-5
MIB
description 3-2
tree hierarchy 3-3
MIB Navigator
exiting 3-1, 3-4
navigation commands 3-3
other commands 3-4
special commands 3-4

N

NETBIOS
Datagram Server 1-38
Name Server 1-38
Network Management
local 1-5
remote 1-5

P

Phys Address 1-17
Proxy ARP 1-39

R

RIP 1-40, 1-55
RIP-2 1-45

S

Selecting a port for configuration
IP 1-36, 1-50
SNMP Community Names
read-only 1-22
read-write 1-22
super-user 1-22
SNMP Traps
enable traps 1-23
trap community name 1-23
trap destination 1-23
Subnet Mask 1-17, 1-19
Sunrpc (NIS) 1-38
System Date 1-16, 1-18
System Time 1-16, 1-18

T

TACACS-Database Service 1-38
Telnet 1-11
Time 1-38
Trivial File Transfer 1-38

U

UDP
Bootstrap Protocol Client 1-38
Bootstrap Protocol Server 1-38
Configuring the Broadcast Redirector 1-38
Domain Name Server 1-38
Host Name Server 1-38
NETBIOS Datagram Server 1-38
NETBIOS Name Server 1-38
port numbers and requested services 1-38
Sunrpc (NIS) 1-38
TACACS-Database Service 1-38
Time 1-38
Trivial File Transfer 1-38

W

WAN Protocols 1-5
WPIMs
WPIM-SYNC A-2